International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:5, 2008

Plug and Play Interferometer Configuration using Single Modulator Technique

Norshamsuri Ali, Hafizulfika, Salim Ali Al-Kathiri, Abdulla Al-Attas, Suhairi Saharudin, and Mohamed Ridza Wahiddin

***Abstract*—**We demonstrate single-photon interference over 10 km using a plug and play system for quantum key distribution. The quality of the interferometer is measured by using the interferometer visibility. The coding of the signal is based on the phase coding and the value of visibility is based on the interference effect, which result a number of count. The setup gives full control of polarization inside the interferometer. The quality measurement of the interferometer is based on number of count per second and the system produces 94 % visibility in one of the detectors.

***Keywords*—**single photon, interferometer, quantum key distribution.

I. Introduction

THE two main goals of cryptography are the encryption of messages to render them unintelligible to third parties and authentication the massage to certify that they have not been modified. These goals can be accomplished if the sender (”Alice”) and recipient (”Bob”) both possess a secret random binary digit (bit) known as ”key”. It is essential that Alice and Bob acquire the key material with a high level of confidence that any third party (”Eve”) does not have even partial information about the random bit sequence. If Alice and Bob communicate solely through classical messages (as opposed to Quantum cryptography), it is impossible for them to generate a certifiably secret key owing to the possibility of passive eavesdropping.

Quantum cryptography or, more precisely, quantum key distribution (QKD) is the new generation of cryptographic system which allows two remote parties (Alice and Bob) to generate a secret key, with privacy guaranteed by quantum mechanics [1], [2]. They transmit a random key securely over an optical fiber connection(also known as Quantum channel). This random key is then used for encryption and decryption of confidential messages, which then can be sent in encrypted form over any non-secured communication channel.

Since the introduction of the BB84 protocol by Bennet and Brassard in 1984 [1] and their first bench-top implementation of QKD over 30 cm of free-space in 1992 [2] extensive efforts by numerous groups [3], [4], [5], [6], [7], [8], [9], [10], [11], [12] has been devoted to extend the QKD distance using optical fibers. The first breakthrough was made by Townsend et al. in 1993 [3] using a phase modulator in a Mach-Zehnder interferometer instead of using polarization based systems. They achieved 10-km transmission of a single photon with high visibility, which was one-order longer transmission than that for polarization-based methods. The next breakthrough was made by using Faraday mirrors to self-align the polarization and to self-balance the path length of the interferometer. This was demonstrated by Muller et al. [9] and they called it the plug and play (P&P) interferometric system. The transmission length was at first limited to 23 km, but recently Stucki et al. have succeeded in extending QKD over 67 km using the P&P system [12].

Norshamsuri is with the Information Security Group, Mimos Berhad, Kuala Lumpur, email: nshamsuri.ali@mimos.my

II. Theoretical review

Quantum key distribution (QKD) scheme can be implemented by sending pulses of polarized light either through freespace transmission or optical fiber. The transmitted light pulses need to be attenuated to a level which allow the transmission of one photon (one bit) at a time in a polarized state. The polarization of light are manipulated according to a certain rules or known as protocols.

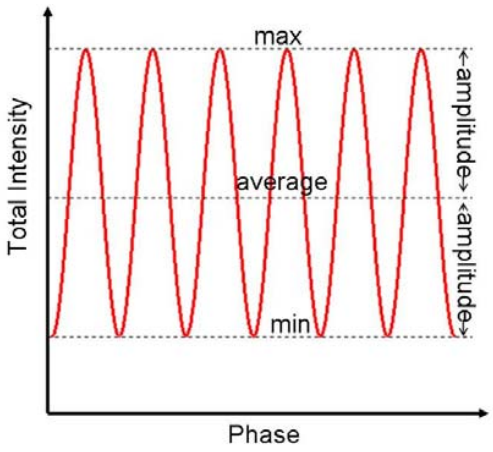

Fig. 1. Visibility in Mach Zehnder interferometer.

Nevertheless, manipulation of light properties such as polarization was found not to be suitable in optical fiber QKD transmission due to polarization scrambling in optical fiber. Instead, the phase of the transmitted photon is used. In this scheme, two communicating parties (Alice and Bob) use single unbalanced Mach-Zehnder interferometers, in which one arm is longer than the other. The interferometers are connected in series by a single optical fiber, and both have phase modulator (PM) which is use to encode the phase onto the light pulses. The light pulses that travel in the interferometer will interfere and as the phase between them is changed, the power or

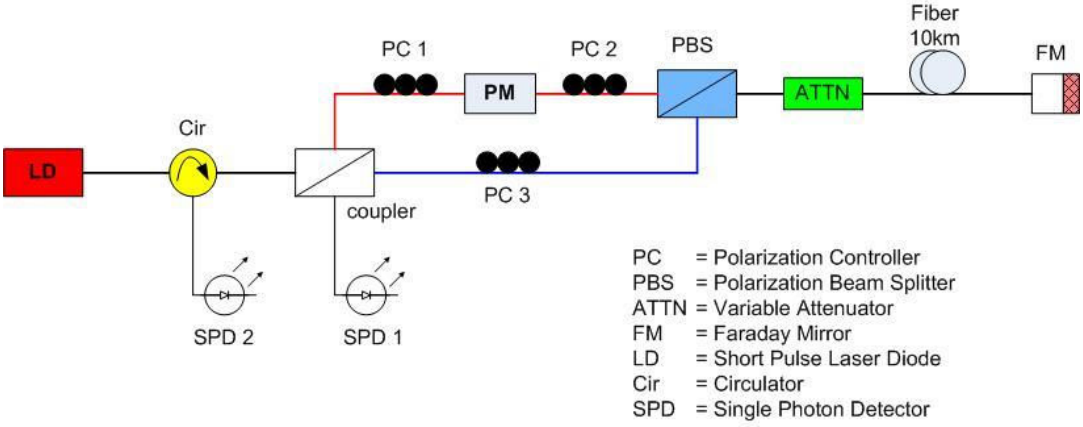

Fig. 2. Schematic of experimental setup used for Plug and Play configuration QKD interferometer at Bob's sides.

intensity (probability in quantum mechanics) of the resulting wave/particle oscillates as shown in Figure 1

The ratio of the size or amplitude of these 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,

$$Visibility_{real} = \frac{amplitude}{average} \tag{1}$$

Alternatively, the above equation can be written as follows;

$$Visibility_{real} = \frac{max - min}{max + min} \tag{2}$$

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;

$$Visibility_{ideal} = \frac{2\sqrt{I_1 I_2}}{I_1 + I_2} \tag{3}$$

where $I_1 I_2$ - Intensities of the optical waves

III. Experimental Configuration

The set-up for the experiment is shown in Figure 2. The set-up represents one of the two interferometers (Alice and Bob's interferometers) in a complete plug and play QKD scheme. In this experiment, only Bob's interferometer is being investigated. The light source for the optical fiber is provided by a short pulse laser diode with a pulse width of 0.3 ns and triggered by an external function generator at a frequency of 100 kHz. Light pulses of 10 us interval is launched into an optical fiber and passes a three port (an input, a common port and an output port) optical circulator (CIR). 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 (longer in length) is connected to a polarization maintaining optical fiber with a length of approximately 1 meter. At both arms, polarization controllers (PC) are installed to control the state of polarization of the light passes through the two arms. The fact that PM is a polarization dependent device, another PC is place right before the PM which function is 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) whose output is connected to a variable optical attenuator (VOA). Due to the unbalanced nature of the interferometer used, the two optical pulses that recombined and leave the PBS will be delayed about 5 ns apart. The optical power (intensity) of the two pulses is then attenuated (to an average power of -108.93 dBm) by the VOA to achieve single photon per pulse. In optical fiber QKD scheme "single photon" are 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.

The attenuated optical pulse then travels through a standard telecommunication grade optical fiber (SMF) of 10 km in length before being reflected back by a Faraday mirror (FM).

IV. Result Discussion

For this experiment, we did some measurement and characterization of the component and equipment before experimental setup.

A. Effect of photodetector dark current toward Single photon detectors efficiency

We began with system detector characterization. The dark count was measured by triggering the detector with an empty pulse. The value of dark count is relative toward the bias

TABLE I
THIS IS THE VALUE OF DARK COUNT PROBABILITY WHEN THE INCREMENT OF GATED TRIGGERING.

Frequency	Count per second	Gates	Normalized
1 kHz	9	1,000	0.009
10kHz	48	10,000	0.0048
100kHz	661	100,000	0.00661
200kHz	2,700	199,999	0.013500068
500kHz	447,374	499,997	0.894753369
1MHz	999,709	1,000,000	0.999709

TABLE II
THIS IS THE PROBABILITY OF AFTER PULSE EFFECT DIFFERENT DEAD TIME OF DETECTOR.

Dead time	Count per second	Frequency
none	33,512	1,000,000
1us	5,350	995,177
2us	3,016	993,968
5us	1,695	991,525
10us	1,272	987,280

voltage. The best bias voltage is used to optimize between dark count probability and detection efficiency since the dark count and efficiency of detector increases when biased voltage increased. The probability of detection is measured as shown below

$$P_{det} = \frac{no.ofcount - no.ofdarkcount}{gatefrequency} \tag{4}$$

The detector efficiency can be measured using this formula by assuming the probability of single photon click is based on Poisson distribution.

$$\begin{aligned}\eta &= \frac{1}{\mu} P_{det} \\ &= \frac{1}{\mu}\left(\frac{no.ofcount - no.ofdarkcount}{gatefrequency}\right)\end{aligned} \tag{5}$$

$$\begin{aligned}P_{det} &= 1 - P_0(\text{no of count}) \\ &= 1 - P_0(1 - P_{dark})\end{aligned} \tag{6}$$

$$P(n) = \frac{\mu^n e^{-\mu\eta}}{n!} \tag{7}$$

$$P_{det} = 1 - e^{-\mu\eta}(1 - P_{dark}) \tag{8}$$

$$e^{-\mu\eta} = \frac{1 - P_{det}}{1 - P_{dark}} \tag{9}$$

$$\eta = -\frac{1}{\mu}\frac{1 - P_{det}}{1 - P_{dark}} \tag{10}$$

We performed intensive study to investigate the relation between power and repetition frequency by conducting measurements at laser source operating at 1.55 μ m and detector side using power meter. We took measurements starting from 10Hz incrementing up to 50MHz. While measuring, power meter showed different power levels of pulse laser with respect to frequency. Increment in number of pulses due to repetition of frequency, will raise number of photon count. Since weak pulse lasers does not actually generate single photon per pulse, the number of photon count in pulses represented by probability or estimated in literature that is calculated by equation (7)

In this experiment setup, the detectors' efficiency is at 25%. This value is lower since the detector in communication region is normally used InGaAs (Indium Gallium Arsenide) material which has higher dark count and after pulse in order to detect at single photon region. This value will reduce the performance of detection by 75% efficiency and reduce the probability to extract the key transferred. In addition, the weak pulses method to generate single photon is already reduce the probability of detection by having only 37% of empty pulse when generating single photon per pulse (μ = 1).

By computing the probability, we found that 37% of pulses are empty and around 26% contains more than one photon. Accumulatively, we will get in average single photons per pulse as shown in Figure 3.

The dark count at the detector also effected the performance of the detectors and also the after pulse effect. Even though, the system is calibrated at the optimum point, but this event still affecting the result. Table 1 and 2 show the dark count probability and after pulse effect in the system at certain condition. The table 1 and 2 show the effect of higher frequency, which increase the probability detection of dark count and the effect of the dead time. In order to maximize the speed of secret key exchange, we have to minimize the dead time as small as possible.

B. Effect of laser repetition rate towards optical power

We can also prove that power levels increases with respect to frequency theoretically by computing single photon energy using the relation [13]

$$E = hf \tag{11}$$

Where h is Plank's constant = 6.626 X 10-34Js and f is the frequency. We can derive another notation we get

$$E = h\frac{c}{\lambda} \tag{12}$$

Since power is the rate of energy delivered, we can write the total energy as

$$P = E \times f_{repitation} \tag{13}$$

By referring to Figure 4 we can see the trend of the average power of total pulse per second increase when the frequency increase. For example, if we take for our repetition frequency at 10 kHz, the average power of total pulse per second is around -55.3 dBm while in 1 MHz measured power to be -35.3 dBm, which yield 20 dB differences. This show, the number of photon per second increase as the frequency increase, since the average power increased. This can be confirmed by calculate the power of the pulses in second as shown in equation (13).

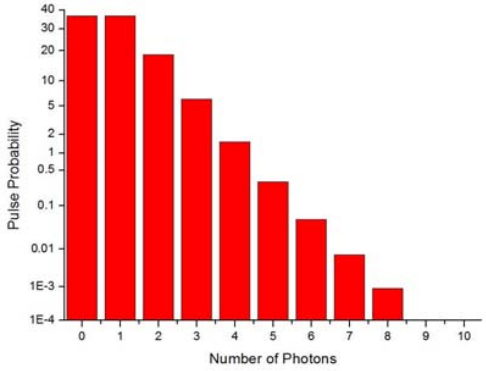

Fig. 3. Probability number of photon arriving per pulse

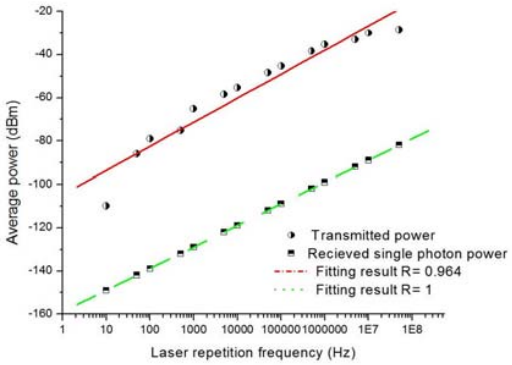

Fig. 4. The average power send and receive in the system which given probability of single photon per pulse.

The result as in Figure 4, is based on measurement and calculation. The power transmitted into the system is measured by using power meter. We can see clearly that the linearity of the curve is not perfect as in measurement result. The result illustrated is acceptable since the red fitting curve (straight line) shows the correlation, R-value is 0.96. This shows that the graph is nearly perfect according to linear increment of power. The second plot shows the calculated power which give single photon per pulse. This curve is base on calculation as shown in equations 8-9. The power meter cannot measure the power level at single photon level, thus calculation is used as estimation to produce single photon source in the system. The value given is based on the transmitted power measured and the power calculated will give correct value.

The difference of average power between these two curves gives the value of distance and acceptance loss for this system. This value can be adjusted accordingly by increasing the power at the transmitting end. In this system, the value between the two curves is the loss in the system due to fiber loss, absorption loss, and component insertion loss.

C. Visibility of Mach-Zehnder interferometer

The visibility value for this experiment was measured based on the effect of photon count per second when varying the phase of pulse. This visibility value is important in order to make sure the configuration setup is perfect during modulation coding. Visibility also shows the correlation of the pulse which represent destructive and constructive event. This event is used as the coding scheme in QKD in order to transfer the key by using single photon or weak pulses. Lower value of visibility will indicate unperfected interference which can contribute more error during key coding. This will result low performance of QKD. The visibility calculation is based on the formula mention in Theoretical review section and elaborate as below.

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{14}$$

$$I = A\cos^2(\theta_1 - \theta_2) + B \tag{15}$$

$$I = A\cos^2(\frac{(x - x_c)}{w}\pi) + B \tag{16}$$

$$I = \begin{cases} A + B, & \text{for} \quad \theta_1 - \theta_2 = n\pi \\ B, & \text{for} \quad \theta_1 - \theta_2 = \frac{n+1}{2}\pi \end{cases} \tag{17}$$

where $n = 0, 1, 2, ...$

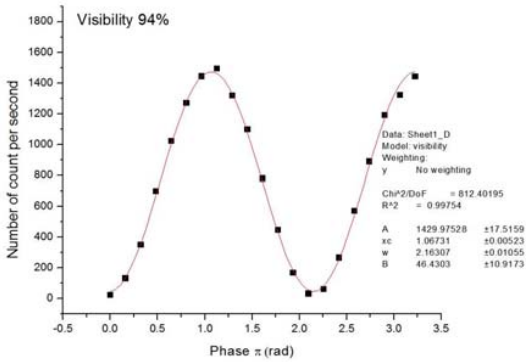

Fig. 5. The interference pattern based on phase coding at detector 1 and curve fitting of the measurement.

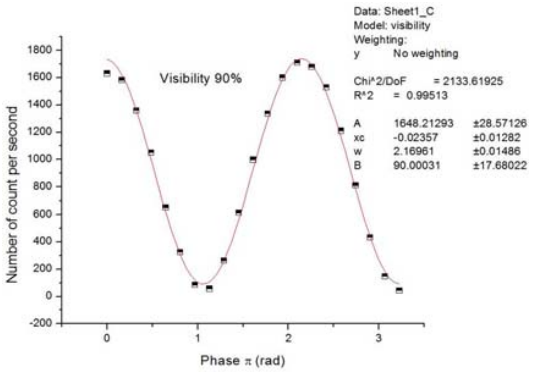

Fig. 6. The interference pattern based on phase coding at detector 2 and the curve fitting of the measurement.

The interference pattern is based on the cosine function as in equation (15).

The value of the interference pattern in Figure 5 and 6 is calculated based on the equation (15). The value A and B obtained by fitting the curve using equation (16). The visibility equation can be summarized from equation (14) - (19).

$$V = \frac{(A+B) - B}{(A+B) + B} \tag{18}$$

$$= \frac{A}{A+2B} \tag{19}$$

Figure 5 and 6 show the result taken from the experimental setup of interferometer at Bob's side. These results are achieved by varying the modulation frequency at one arm and maintain the other arm to see the effect of interference. The interference of the light gives the value of photon counting in a second. Figure 5 shows interference pattern result for detector 1 and Figure 6 show interference pattern result for detector 2.

In this experiment, we found that the destructive and constructive event has changed from the normal interferometer. The event of constructive should happen at the first detector has changed to the second detector and vice versa. This shows the effect of faraday mirror in this setup which reflecting the light by rotating the polarization of light into it's orthogonal polarization. This event has changed the normal phenomena of Mach-Zehnder interferometer. The constructive interference should occur at detector 1 if the phase between the pulse is 0 and the destructive interference at detector 2. In this setup the event is vise versa as we can see at Figure 5 and Figure 6 the phenomena has shift by π rad.

Equation (19) will give the value of visibility for both detectors, which show the performance of the setup and phase coding in the system. From the equation, we found that the visibility for the curve is 94% for the first detector and 90% for the second detector

There are some limitations in this system, which contributes to visibility performance for example, dark counts and after pulse which we have already discussed in subsection A.

Another limitation that reduces the performance of the visibility in this experiment are modulator and used of single mode fiber. As mention above, the modulator used in this experiment is polarization dependent. In this experiment setup, the light has to go through in both directions of input and output. This light has different polarization when enter from input and also output of the modulator. Since this modulator is polarization dependent, the coding of the pulse will effect if the polarization of the light is not matched with the modulator.

The single mode fiber has increased the uncertainty of polarization where polarization keeps on changing towards environment effect. This will affect the performance of modulator and create unperfected combine and splitting pulse at PBS since the polarization state is uncertain towards environment.

Even though, there are limitations in the system, we manage to get good result in this experiment. The 94% of visibility indicates good performance of interferometer correlation which shows good quality of key coding. The Quantum Bit Error Rate (QBER) can be estimated by using the value of visibility. This will give the estimation of the QBER value which can be calculated by $QBER = \frac{1-V}{2}$. Thus, result obtain is about 3%. This show the system design gives better performance in the system even though they have certain limitation in the system.

V. Conclusion

The configuration scheme of plug and play QKD by using two-way single photon traveling improve the interference visibility. The result proves the robustness towards fiber installation and environment effects. The quality of the system may improve if the Bob's interferometer uses all polarization mode fiber in the system.

Acknowledgment

We wish to acknowledge the support of the lab community in giving views and ideas. We are also grateful to Prof Hugo Zbinden for his helpful support to our team and Dr. Suryadi for his commitment consultation to the team. ....

References

[1] Bennett, C.H., and Brassard, G., *Quantum cryptography: Public key distribution and coin tossing* (Proc. Int. Conf. Comput. Syst. Signal Process, Bangalore, 1984, pp. 175-179).

[2] Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J.,*Experimental quantum cryptography* (J. Cryptol., 1992, 5, (3)).

[3] Townsend, P.D.; Rarity, and J.G.; Tapster, P.R, *Single photon interference in 10 km long optical fibre interferometer* (Electronics Letters, 1993, 29, pp. 634-635).

[4] Muller, A.; Breguet, J.; and Gisin, N, *Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km* (Europhysics Letters, 1993, 23, pp. 383-388).

[5] Townsend, P.D.; Rarity, J.G.; and Tapster, P.R.,*Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel* (Electronics Letters, 1993, 29, pp. 1291-1293).

[6] Franson, J.D. and Jacobs, B.C, *Operational system for quantum cryptography* (Electronics Letters, 1995, 31, pp. 232-234).

[7] Marand, C., and Townsend, P.D *Quantum key distribution over distances as long as 30 km* (Optics Letters, 1995, 20, pp. 1695-1697).

[8] Muller, A., Zbinden, H., and Gisin, N *Quantum cryptography over 23 km in installed under-lake telecom fibre* (Europhysics Letters, 1996, 33, pp. 335-339).

[9] A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H., and Gisin, N *Plug and play" systems for quantum cryptography* (Applied Physics Letters, 1997, 70, pp. 793-795).

[10] Zbinden, H., Gautier, J.D., Gisin, N., Huttner, B., Muller, A., and Tittel, W *Interferometry with Faraday mirrors for quantum cryptography* (Electronics Letters, 1997, 33, pp. 586-588).

[11] Ribordy, G., Gautier, J.D., Gisin, N., Guinnard, O., and Zbinden, H *Automated 'plug and play' quantum key distribution* (Electronics Letters, 1998, 34, pp. 2116-2117).

[12] Stucki, D., Gisin, N, Guinnard, O., Ribordy, G., and Zbinden, H *Quantum Key Distribution over 67 km with a plug & play system* (quant-ph/0203118, 2002).

[13] Palais, Joseph C *Fiber optic communications, 4th Ed* (Prentice Hall, 1998).

Norshamsuri Researcher, Quantum Cryptography Group, Information Security Lab, Mimos Berhad. He received his B.Eng (Hons) degree in Electric Electronics Engineering from University of Tenaga Nasional, Malaysia in 2002. He completed his M.S degree in Optical Communication from University of Putra, Malaysia in 2005, while he joined Photonics Laboratory University of Putra as Research Assistant conduct his research on optical amplifier, opto-electronics devices and optical access communication system. From 2005, he is Lecturer at British Malaysia Institute, University of Kuala Lumpur. Later in 2006, he joined Mimos Berhad, Malaysia to work on quantum cryptography. Currently he leading fiber based quantum key distribution project. His research interest include quantum communication, quantum cryptography, weak laser pulse, single photon detector and photonics entanglement.

Hafizulfika Assoc. researcher, Quantum Cryptography Group, Information Security Lab, Mimos Berhad. He received his degree in Computer and Communication System Engineering from University of Putra Malaysia in 2002. He starts his career in optical fiber field as research assistant at Photonics laboratory University of Putra Malaysia and involved optical fiber industries and consultant at Significant Technologies until 2006 as Engineer. Later in 2007, he joined Mimos Berhad, Malaysia to work on quantum cryptography. Currently he involved with fiber based quantum key distribution project and his research interest is quantum communications.

Salim Research Assistant, Quantum Cryptography Group, Information Security Lab, Mimos Berhad. He received his B.Eng (Hons) degree in Computer & Information Engineering from International Islamic University (IIU), Malaysia in 2005. Currently he is pursuing his M.S. in International Islamic University under the collaboration with MIMOS Berhad. His research interest includes quantum communication, quantum cryptography.

Abdulla Research Assistant, Quantum Cryptography Group, Information Security Lab, Mimos Berhad. He received his B.Eng (Hons) degree in Computer & Information Engineering from International Islamic University (IIU), Malaysia in 2004. During his undergrad studies, he was an Assistant Lecturer at International Islamic University. Later in 2005, he joined the IT Department in King Abdulaziz University, Saudi Arabia. Currently he is pursuing his M.S. in International Islamic University under the collaboration with MIMOS Berhad. His research interest includes quantum communication, quantum cryptography, eavesdropping strategies.

Suhairi Saharudin PhD. joined MIMOS Berhad in 2005. Prior to that, he was a researcher at SIRIM Berhad for 12 years. During the 12 years research in SIRIM Berhad, his interest was in Optical fiber communication, optical fiber sensors and industrial lasers. He is now a Staff Researcher in MIMOS Berhad undertaking researcher activities in Quantum Key Distribution. He obtained his PhD in Computer and Communication Systems Engineering from Universiti Putra Malaysia.

Mohamed Ridza Wahiddin received the higher doctorate degree, Doctor of Science (DSc) from The University of Manchester for his contributions to the advancement of knowledge in the field of Quantum Optics in 2004. Presently, he is the Head of Information Security Cluster at MIMOS BERHAD. Prof. Ridza has delivered invited talks in several local and overseas conferences, has five patents filed and has co-authored three scientific books. He was MIMOS Best Innovator for 2007.