Iraqi J. Laser, Part A, Vol. 8, pp. 29-35 (2009)

IRAQI JOURNAL OF LASER

Real Time Quantum Bit Error Rate Performance Test for a Quantum Cryptography System Based on BB84 protocol

Ahmed I. Khaleel **Shelan Kh. Tawfeeq**

Institute of Laser for Postgraduate Studies , University of Baghdad, Baghdad, Iraq

(Received 5 October 2009; accepted 5 January 2010)

Abstract: In this work, the performance of the receiver in a quantum cryptography system based on BB84 protocol is scaled by calculating the Quantum Bit Error Rate (QBER) of the receiver. To apply this performance test, an optical setup was arranged and a circuit was designed and implemented to calculate the QBER. This electronic circuit is used to calculate the number of counts per second generated by the avalanche photodiodes set in the receiver. The calculated counts per second are used to calculate the QBER for the receiver that gives an indication for the performance of the receiver. Minimum QBER, 6%, was obtained with avalanche photodiode excess voltage equals to 2V and laser diode power of 3.16 nW at avalanche photodiode temperature of -10°C.

Keywords: Quantum cryptography, Avalanche photodiode, Quantum bit error rate.

Introduction

The very important reason behind the use of cryptography is to provide a high degree of secrecy and to ensure that any sensitive information when it has to be exchanged between two parties, no unauthorized third party can get access to the content without being noticed. The one-time pad as considered to be a classical cryptographic method, proved to be secure, if and only if the key has been deployed securely. Yet, this task cannot be provably accomplished by classical means [1].

The basic idea of the one-time pad is that the secret key is purely random, as long as the message itself, and used only once. But also it has a serious drawback, it presupposes that random string of secret, a key, is shared between Alice and Bob before the actual transmission of the message. So by the introduction of the one-time pad the problem of secure communication is shifted to the problem of secure key distribution. This is called the key distribution problem. In top secret applications, key distribution is often done by trusted couriers [2].

The most important detail in quantum cryptography is that it deals with the smaller unit of energy in the universe ever found yet which is called photon. By arranging some properties of the photon it can be used to transfer information and since it is the smallest unit of energy so it cannot be divided and this is the very important property that gives the quantum cryptography its power [3].

The BB84 protocol [3] deals with a cryptographic system that consists of Alice (the sender) which consists of four laser diodes (LD) plus optics required to direct the laser beam to the receiver and Bob (the receiver) and they are communicating over a quantum channel which was a free space in the very first experiment when Bennett and Brassard implemented it. Also they used another public channel for public conversation between Alice and Bob [3]. Table

(1) summarizes the BB84 protocol. The schematic diagram of a quantum cryptography system based on BB84 protocol is shown in Figure (1).

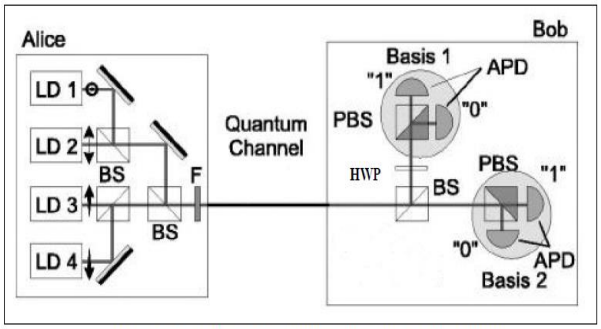

Fig. (1): Schematic diagram for a typical quantum cryptography system based on BB84-protocol [4]

Bob's part is constructed from four avalanche photodetectors (APDs) to detect the four different polarization states (H, V, +45°,-45°). The detectors are arranged with additional optical elements (beam splitter, polarized beam splitter, half-wave plate(HWP) to form the optical setup of Bob model. One of the most widely used APD is the (Perkin Elmer C30902)[4] which is silicon APD used for single photon detection.

To estimate the error produced in the quantum key distribution (QKD) system, a parameter called Quantum Bit Error Rate (QBER) must be calculated. This parameter is calculated when the sifted key is obtained. The sifted key represents the remaining shared secret bits between Alice and Bob (Table (1)). In principle it is defined as the ratio of wrong bits to the total number of bits received, it can be expressed as a function of rates as [5, 6]:

$$QBER = \frac{N_{wrong}}{N_{right} + N_{wrong}} = \frac{R_{error}}{R_{sift} + R_{error}} \cong \frac{R_{error}}{R_{sift}} \quad (1)$$

(when $R_{error} \langle\langle R_{sift}$) The sifted key corresponds to the cases in which Alice and Bob made compatible choices of bases, hence its rate is half that of the raw key [5]:

$$R_{sift} = \frac{1}{2} R_{raw} = \frac{1}{2} q f_{rep} \mu t_{link} \eta \quad (2)$$

where

q: factor ≤ 1 (typically 1 or 0.5)

f_{rep} : pulse rate

μ: the mean number of photons per pulse

t_{link} : the probability of a photons arriving at the analyzer

η : the probability of the photon's being detected

The error rate R_{error} can be identified through three different contributions that are [5]:

$$R_{opt} = R_{sift} p_{opt} = \frac{1}{2} q f_{rep} \mu t_{link} p_{opt} \eta \quad (3)$$

where

p_{opt}: the probability of a photon's going to the wrong detector

$$R_{\det} = \frac{1}{2}\frac{1}{2} f_{rep} p_{dark} n \quad (4)$$

where

p_{dark}: the probability of registering a dark count per time window and per detector

n: the number of detectors

The two factors of ½ are related to the fact that a dark count has a 50% chance of happening when Alice and Bob have chosen incompatible bases (and is thus eliminated during sifting) and a 50% chance of occurring in the correct detector.

$$R_{acc} = \frac{1}{2}\frac{1}{2} p_{acc} f_{rep} t_{link} n \eta \quad (5)$$

where

p_{acc}: the probability of finding a second pair within the time window, knowing that a first one was created

QBER can now be expressed as [5]:

$$QBER = \frac{R_{opt} + R_{\det} + R_{acc}}{R_{sift}} \quad (6)$$

$$= p_{opt} + \frac{p_{dark} n}{t_{link} \eta 2 q \mu} + \frac{p_{acc}}{2 q \mu} \quad (7)$$

$$= QBER_{opt} + QBER_{\det} + QBER_{acc} \quad (8)$$

where

$QBER_{opt}$: this factor is independent of the transmission distance (it is independent of t_{link}). It can be considered as a measure of the optical quality of the setup, depending only on the polarization or interference fringe contrast

$QBER_{\det}$: this factor increases with distance, since the dark-count rate remains constant while

the bit rate goes down like t_{link} . It depends entirely on the ratio of the dark-count rate to the quantum efficiency.

$QBER_{acc}$: this factor is present only in some two-photon schemes in which multiphoton pulses are processed in such a way that they do not necessarily encode the same bit value.

BB84 QKD implemented with ideal devices would give QBER = 0 if there are no eavesdropping attacks. If eavesdropping attacks exist in the quantum channel, the QBER at Alice's and Bob's sifted keys will increase. Non-zero QBER can also be attributed to imperfect devices. Since QBER resulted from eavesdropping attacks and QBER due to imperfect devices are indistinguishable, Alice and Bob must always assume that errors in their sifted key are due to eavesdropping attacks to the quantum channel [7].

In order to check the performance of Bob module, i.e., optical alignment is set as exact as it can be and the detectors are working with their corresponding angles, a performance test to Bob side only is made. This is done by putting a laser diode with same beam parameters of the laser diode used by Alice in front of Bob module. The output beam is sent through an attenuating filter to reduce it's output power then the output beam is polarized at (0) degree using a polarizer. The output beam from the polarizer is sent through a half-wave plate (HWP) in order to rotate the output beam from 0 to 180 degree. The final beam is sent to Bob setup and simultaneously when changing the angle of the HWP. The number of counts that are detected by the detectors are recorded and plotted in real time for every 1 second. If the alignment was set precisely, the detectors behavior will respond to the variation of the HWP angle, which means that for example for HWP angle with 45 degree, the detection of the vertical detector must be maximum and the detection of the horizontal detector must be minimum, whereas the other two detectors (-45°,+45°) will have in-between detections QBER for each detector can be calculated using the following formula [8]:

$$QBER_{|H\rangle} = \frac{n_V|H\rangle}{n_V|H\rangle + n_H|H\rangle} \qquad (9)$$

where,

$n_i|\psi\rangle$: The count rates of detector i for the incident polarization state $|\psi\rangle$

QBER can be deduced from the ratio of the counts in the H-detector produced from V-polarized pulses versus the counts produced from the same number of H-polarized pulses. the same rule is applied for the other three directions using the formula [9]:

$$QBER_{|H\rangle} = \frac{n_H|V\rangle}{n_H|H\rangle} \qquad (10)$$

The dark count of the APD includes the counts thermally generated by the APD itself and the counts due to ambient light. To avoid this ambient light, the APD must be carefully shielded using dark screens and pinholes. Since the dark counts are independent of the polarization or wavelength or the alignment of the system, it can be subtracted from the overall counts when calculating the QBER [10].

Figure (2) shows the characterization of the polarization analysis setup with highly linearly polarized light. Count rates of the individual single-photon detectors as a function of the polarization angle of the incoming light are recorded [8].

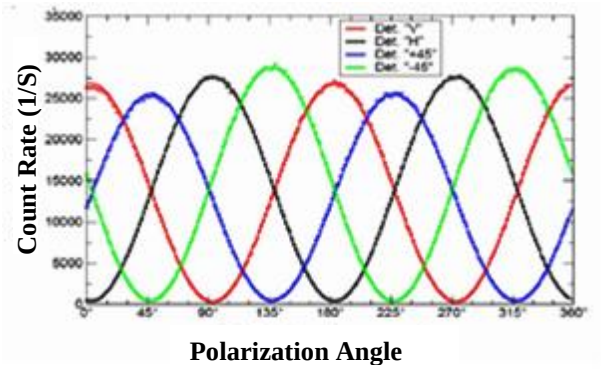

Fig. (2): Variation of detectors count rates with variation of the HWP angle [9]

Experimental Setup

The receiver is constructed from four avalanche photodiodes (APDs) working in the Geiger mode. In this mode, the device is biased above breakdown voltage V_b by an amount ΔV which is called the excess voltage V_E and remains at this value until a breakdown occurs [11]. The detectors are connected to a passive quenching circuit (PQC). The output of the passive quenching circuit is then amplified and finally applied to a comparator to generate a digital signal (TTL signal). This digital signal is then fed to the counter circuit that was implemented. Figure (3) shows the block diagram of an APD receiver.

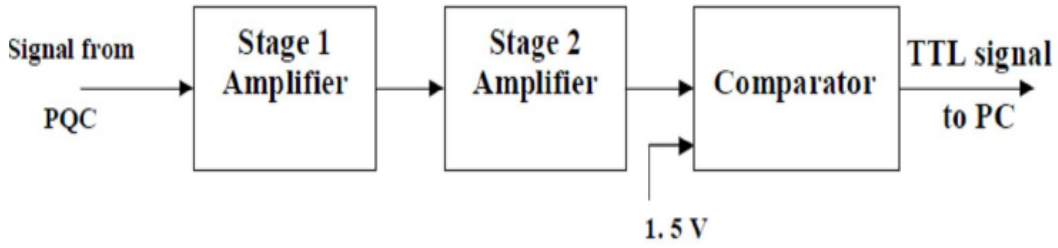

Fig.(3): Block diagram of APD receiver

To calculate the QBER at Bob side of a quantum cryptography based on BB84 protocol that uses polarization encoding, some optical elements must be added and optical arrangement must be set. The extra added elements are a laser diode with specification similar to that used at Alice side (λ=650 nm), an optical filter with (Transmitivity T=0.4% @ 650 nm) which gives an LD output power of (0.56, 1,84 and 3.16) nW, one polarizer set at 0° and one half wave plate (HWP).

The schematic diagram of the optical setup is shown in Figure (4).

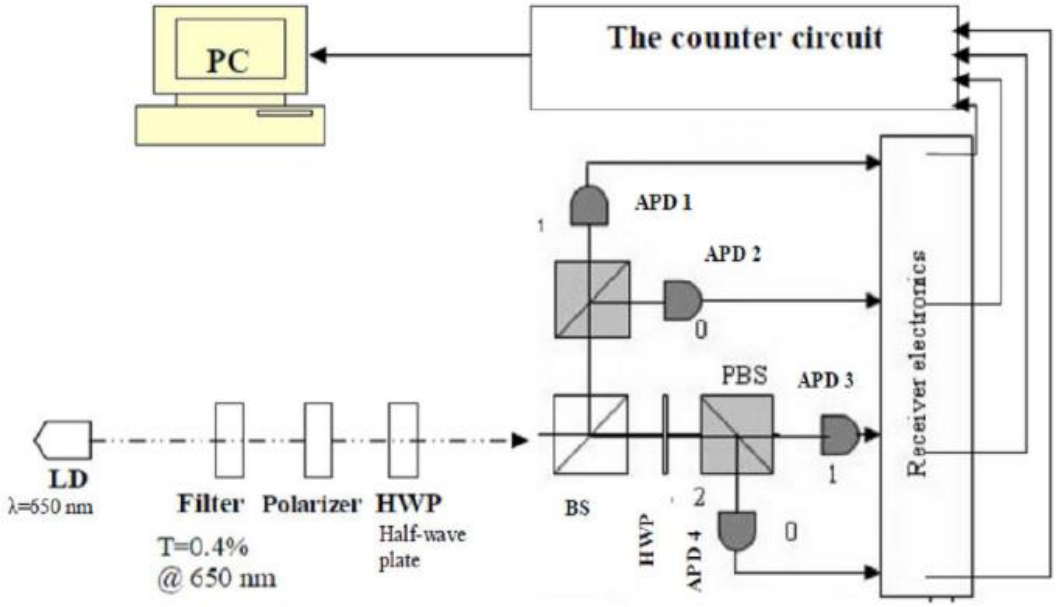

Fig. (4): Optical setup to calculate QBER

QBER was calculated for 2,5 and 7 V APD excess voltage, for each value the LD output power was equal to 0.56,1.84 and 3.16 nW. The HWP is rotated from 0° to 90° so the transmitted beam is rotated from 0° to 180°. The transmitted light from the HWP is sent to the receiver so that the response of the detectors can be observed. This is done by recording the number of counts for each detector using MATLAB program at the same time at which the HWP is rotated. The detectors response will vary due to the variation in the polarization of the light beam. This variation in the detectors response will be plotted directly using MATLAB program. Equation (9) was applied to calculate the QBER.

Results and discussion

The shape of the response of the APDs varies due to the variation in the polarization of the incoming laser light. This variation in the

response is a result of the optical arrangement of the receiver which causes that each APD's detection will be maximum at its appropriate angle and minimum at it's orthogonal angle.

The APD's detection will be in-between value for the other angles. For example the horizontal detector will be maximum when the polarization of the incoming light is 0° and it will be minimum when the polarization becomes 90°. The number of dark counts of an APD is affected by temperature of the APD itself. It increases with temperature which causes the QBER to be increased.

Also the detection of the APD for the LD light increases with the power of the incoming laser light which results the QBER to be decreased, this may reflects the fact that the dark-count contribution (which is random) to the QBER becomes less significant if the number of photon-counting events gets more and more dominant than the random dark counts of the single photon counting modules.

The effect of increasing the excess voltage can be seen on the number of dark counts as it increases with the excess voltage also the detection efficiency of the APD increases with V_E. Figure (5) shows a comparison of APDs response at various conditions.

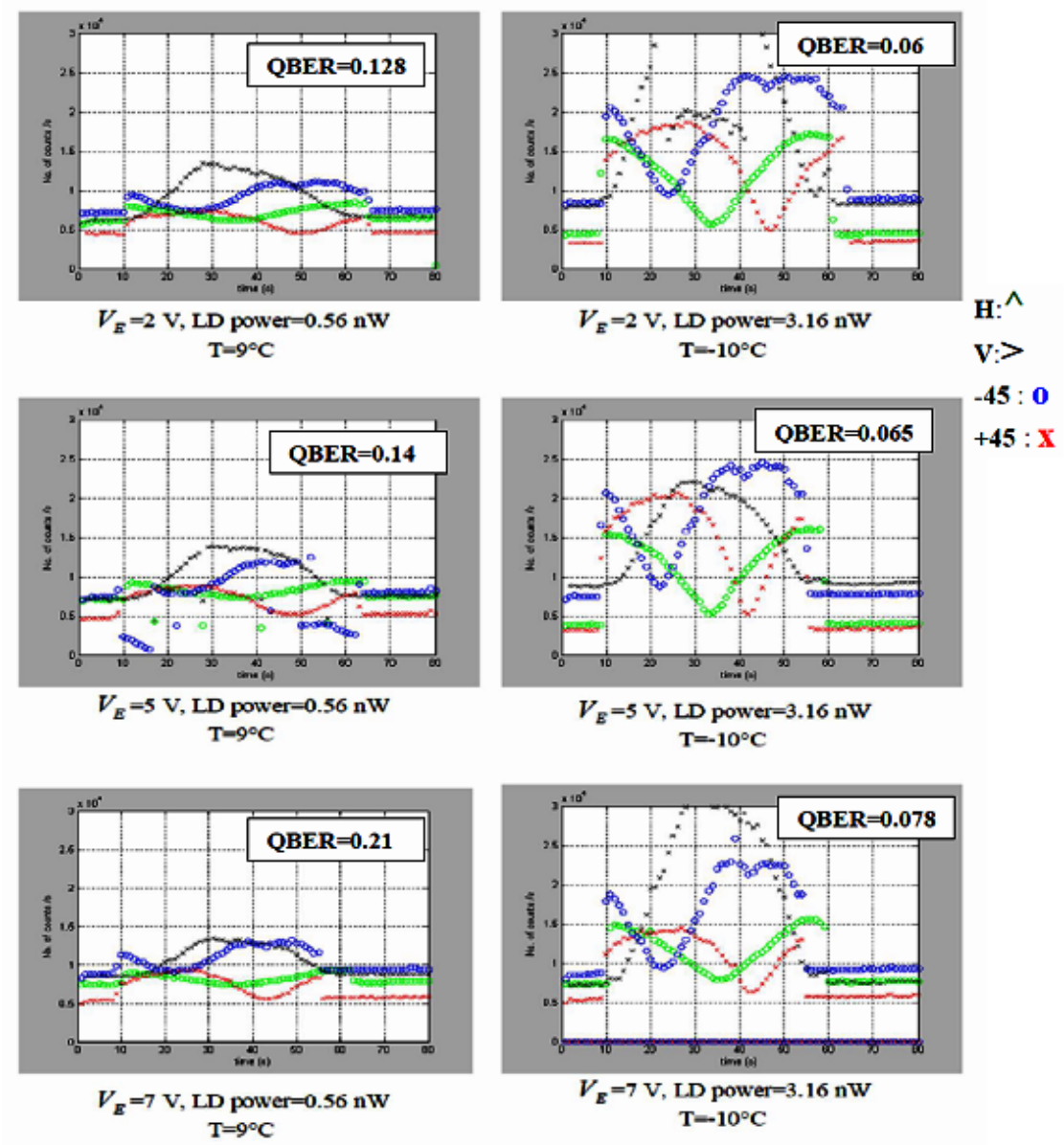

Fig. (5): APDs count at various conditions

Any two adjacent figures shows the response of the APDs when working at the same V_E while increasing the LD power (from 0.56 nW to 3.16 nW) and decreasing the APDs temperature (from 9°C to -10°C) which causes an improvement in detection of the APDs which leads to a decrease in the QBER values. The best result (QBER=6%) was obtained with V_E of 2V and LD power of 3.16 nW when the APD temperature was -10°C.

There are many international experiments made in this field in order to calculate QBER. Some of the calculated QBER values can be mentioned like QBER 0.85% [8], QBER 1.2% [9] and QBER 4.6% [10].

The improvement in the response of the APDs does not necessarily improves the QBER as a value but the improvement can be noticed in the shape of the response curve in the graphs of the number of counts per second. This is because the number of photon-counting events overcomes the effect of the dark counts.

Figure (6) shows a comparison of calculated QBER at T=9°C for different values of V_E.

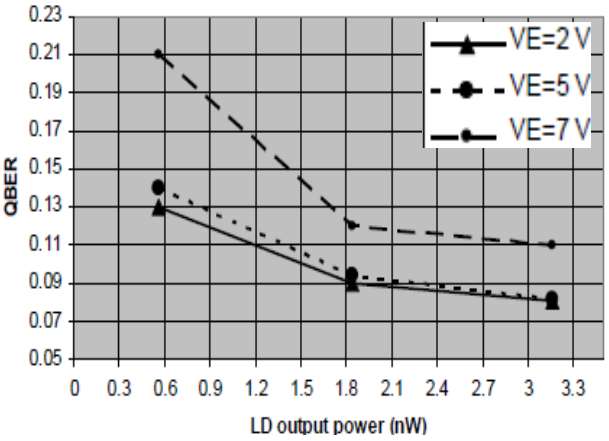

Fig.(6): A comparison of calculated QBER at T=9°C

From Figure (6), the QBER increases when V_E increases due to the increment in the dark count level for the same LD power. Also increasing the LD power results an improvement in the detection with the APDs so the number of the detected signal will increase and so the calculated QBER will decrease .

As seen in Figure (7) the effect of operating the system at low temperature (-10) has a direct impact on the dark counts thermally generated by the APDs. The dark counts decrease as the temperature decreases resulting in a decrease in the calculated QBER.

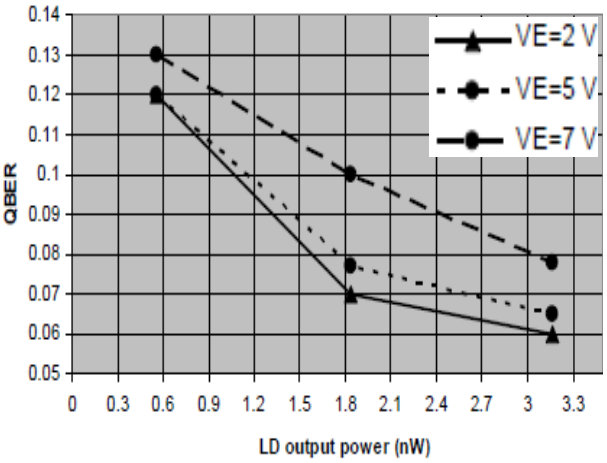

Fig. (7): A comparison of calculated QBER at T =-10°C

For Figures (6) & (7), the effect of working with higher LD power is clearly noticed on the calculated QBER values. This effect is an improvement in the QBER values as the signal that detected by the APDs increases and in the same time the level of dark counts stays constant. Also increasing the excess voltage improves the response of the APDs because it increases the detection efficiency of the APDs but at the same time the dark count also increases. The selection of the value of the excess voltage must be carefuly chosen in order to compromise between the detection efficiency and the dark count.

References

1. H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer and H. Weinfurter "Free Space Quantum Key Distribution: Towards a Real Life Application" Fortschr. Phys. **54**, No. 8 – 10, 840 – 845 (2006).

2. H. Lo and N. Lutkenhaus "Quantum Cryptography: from Theory to Practice" Web-page Quantum Physics 2007 http://arxiv.org/abs/quant-ph/0702202V313Mar2007

3. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", International Conference on Computers, Systems and Signal Processing, Bangalore, **175** (1984).

4. Silicon Avalanche Photodiodes datasheet

5. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum Cryptography", Review of Modern Physics, **74**, 145 – 195, (2002).

6. J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro and J. G. Rarity "Low cost and compact quantum key distribution" New Journal of Physics, **8**, 249 (2006).
7. Y. Kim, Y. Jeong, and Y. Kim "Implementation of polarization-coded free-space BB84 quantum key distribution", Laser Physics, **18**, No. 6, 810–814 (2008).
8. T. Schmitt_Manderbach "Long Distance Free-Space Quantum Key Distribution " PhD. Dissertation, Technical University of Munich (2007).
9. S. Chiangga, P. Zarda, T. Jennewein and H. Weinfurter "Towards practical quantum cryptography" Appl. Phys. B **69**, 389–393 (1999).
10. Beveratos, R. Brouri, T. Gacoin, A. Villing, J. Poizat and P. Grangier, "Single Photon Quantum Cryptography", Physical Review Letters, **89**, No. 18, (187901-1) – (187901-4) (2002).
11. S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche Photodiodes and Quenching Circuits for Single–Photon Detection", Applied Optics, **35**, No. 12, 1956-1976 (1996)

اختبار معدل خطأ الوحدة الكمية لمنظومة تجفير كمي في الوقت الحقيقي

احمد اسماعيل خليل **شيلان خسرو توفيق**

معهد الليزر للدراسات العليا, جامعة بغداد ، بغداد ، العراق

الخلاصة في هذا العمل ,تم اختبار اداء المستلم في منظومة تجفير كمي المعتمدة على بروتوكول BB84 وذلك من خلال احتساب معدل خطأ الوحدة الكمية للمستلم. من اجل تطبيق هذا الاختبار فان مجموعة من البصريات تم ترتيبها وكذلك تم تصميم دائرة الكترونية من اجل احتساب معدل خطا الوحدة الكمية. تستخدم هذه الدائرة الالكترونية لاحتساب عدد العدات في الثانية المتولدة بواسطة الكواشف الضوئية الثنائية ذات الانهيار المضاعف الموجودة في المستلم. ان عدد العدات المحتسبة في الثانية تستخدم في حساب معدل خطأ الوحدة الكمية للمستلم والذي يعطي اشارة عن اداء المستلم. اقل معدل خطأ وحدة كمية تم الحصول عليه هو 6% وذلك عند تثبيت مقدار الجهد الكهربائي الزائد للكواشف الضوئية الثنائية ذات الانهيار المضاعف عند 2 فولط وكانت قدرة الدايود الليزري المستخدم هي 3,16 نانو وات وكانت درجة حرارة الكواشف الضوئية الثنائية ذات الانهيار المضاعف هي (10−°).