Iraqi J. Laser, Part A, Vol. 9, No.2, pp.1-8 (2010)

IRAQI JOURNAL OF LASER

Generation of Weak Coherent Pulses for Quantum Cryptography Systems

Fuad A. Yassien [1] **Shelan K. Tawfeeq** [2] **Ahmed I. Khalil** [2] and **Farah R. Aziz** [2]

(1) *Computer Center-University of Baghdad, Baghdad, Iraq*
(2) *Institute of Laser for Postgraduate Studies, University of Baghdad, Baghdad, Iraq*

(Received 5 July 2010; accepted 10 October 2010)

Abstract: This work is a trial to ensure the absolute security in any quantum cryptography (QC) protocol via building an effective hardware for satisfying the single-photon must requirement by controlling the value of mean photon number. This was approximately achieved by building a driving circuit that provide very short pulses (≈ 10 ns) for laser diode -LD- with output power of (0.7-0.99mW) using the available electronic components in local markets. These short pulses enable getting faint laser pulses that were further attenuated to reach mean photon number equal to 0.08 or less.

Keywords: quantum cryptography, weak coherent pulses, and single photon sources.

Introduction

The first provable unconditional security between communication parties is quantum cryptography. According to the uncertainty principle in quantum mechanics, the quantities of two conjugate observables, i.e., the polarization of a photon in the rectilinear and diagonal basis, can never be measured precisely and simultaneously. The measuring of polarization of a photon, the choice of the measurement basis, affects all the subsequent measurements. Using a pair of orthogonal states, 1 and 0 can be encoded in a single photon. If two conjugate pairs of orthogonal states are chosen randomly during the encoding, the measurements of an eavesdropper will cause perturbations to the photons states with a probability of 50%.

Therefore the presence of the eavesdropper can be detected. This is the basic idea of the BB84 protocol [1] of quantum cryptography, which gives unconditional security in communication [2]. Instead of "real" single photons attenuated laser pulses are commonly used. Since the mean number of the photons in laser pulses follows the Poissonian distribution, there is always a non-vanishing probability to find two or more photons within a laser pulse, even though the average photon number per pulse is set far below unity. This gives rise to a potentially important security leakage known as photon number splitting attack. For a quantum channel with high loss it is possible for an eavesdropper to share almost all the information without being detected. Therefore the implementations of quantum cryptography with attenuated laser pulses are restricted by distance [2].

The basic quantum key distribution (QKD) security proofs require pure single-photon transmission, the use of faint laser pulses associated to Poissonian photon number statistics is an open door to information leakage towards an eavesdropper. There are nevertheless several ways to guarantee unconditional security for practical setups which employs weak coherent pulses (WCPs) instead of pure single-photon pulses. Increasing the attenuation on the quantum channel in order to limit the presence

of pulses containing two photons or more is a simple solution. In practice, the information-encoded laser pulses should correspond to a mean number of photon per pulse well below unity, putting a severe limitation on the maximum transmission distance for which unconditional security of the key can be guaranteed. To improve security of long-distance QKD, refined protocols like "differential phase-shift" QKD and "decoy-state" QKD, have been proposed. [3].

Photon number statistics

Under certain conditions, the arrival of photons may be regarded as the independent occurrences of a sequence of random events at a rate equal to the photon flux, which is proportional to the optical power. For coherent light with constant optical power (P), the corresponding mean photon flux is[4], of registration of the photons are random as shown in Figure 1.

$$\Phi = P/h\upsilon(\text{photon/ s}) \qquad (1)$$

where,
h: is the Planck's constant (6.626×10-34 J.s),
υ: is the frequency of emitted light in Hz.
Φ is also constant, but the actual times

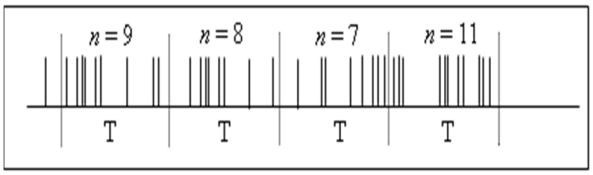


Fig. (1): Random arrival times of photons within intervals of duration T [4].

The number of detected photons within time T is *n*. The mean value of the number of photons (*n*) is,

$$\mu = \Phi\, T = PT/h\upsilon \qquad (2)$$

The expression for the probability distribution p(*n*) can be derived under the assumption that the registrations of photons are statistically independent, the result is Poisson distribution[4].

$$p(n) = \frac{\mu^n}{n!} e^{-\mu}, \quad n = 0,1,2 \qquad (3)$$

Figure 2 shows the Poisson distribution for several values of μ. The curves become progressively broader as μ increases [4].

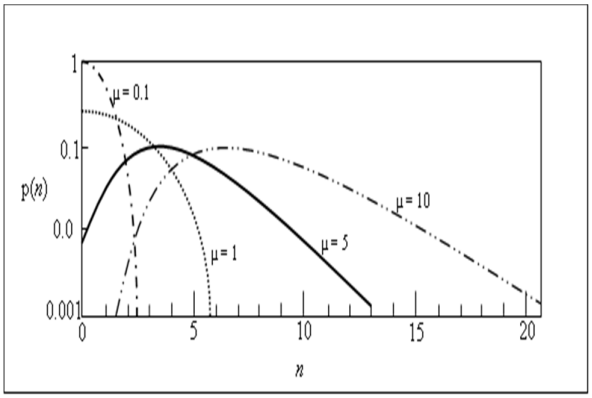


Fig. (2): Poisson distribution p(n) of the photon number n [4]

If T is divided into N of sub-intervals of sufficiently small duration T/N, where N is assumed to be very large so that each interval carries one photon with probability, **p= μ / N**, and no photons with probability, **1-p** .

The probability of finding n independent photons in the N intervals, like the flips of a coin, follows the binomial distribution [4],

$$p(n) = \frac{N!}{n!(N-n)!} p^n (1-p)^{N-n}$$

$$= \frac{N!}{n!(N-n)!} \left(\frac{\mu}{N}\right)^n (1-\frac{\mu}{N})^{N-n} \qquad (4)$$

If $N \to \infty$, $N!/(N-n)!\ N^n \to 1$, and $[1-(\mu/N)]^{N-n} \to e^{-\mu}$ $e^{-\mu}$, so that Equation 3 is obtained [4].

For μ=0.1 the Poisson distribution is shown in Figure 3 [5].

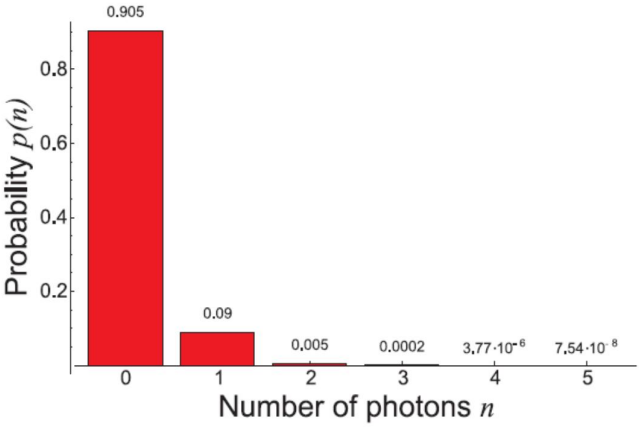


Fig. (3): Poisson distribution for $\mu = 0.1$. It shows the probability that a pulse of a coherent beam contains *n* photons [5].

Figure 3 is drawn by applying Equation 3 for μ equals to 0.1. For μ = 0.2 with various values of n, p(n, μ) values are listed in Table 1

Table (1): Results of applying Equation 3 for μ=0.1 and 0.2 (3)

μ	P(0, μ)	P(1, μ)	P(2, μ)	P(3, μ)	P(4, μ)	P(5, μ)
0.1	0.9048	0.09	0.0045	0.00015	0.00000377	0.0000000754
0.2	0.8187	0.1637	0.0164	0.0011	0.000055	0.0000022

Single photon sources can be tested by using Hanbury-Brown-Twiss (HBT) as in the experimental setup shown in Figure 4. In photon language, the two detectors in HBT experiment count the number of photons transmitted through or reflected from the beam splitter. A series of measurements in which the numbers n_1 and n_2 of photons counted by the two detectors during a constant brief time interval are recorded. Each detector registers the same average number n_3 of counts if the series of identical experiments is sufficiently long [6],

$$\langle n_1 \rangle = \langle n_2 \rangle = n_3 \qquad (5)$$

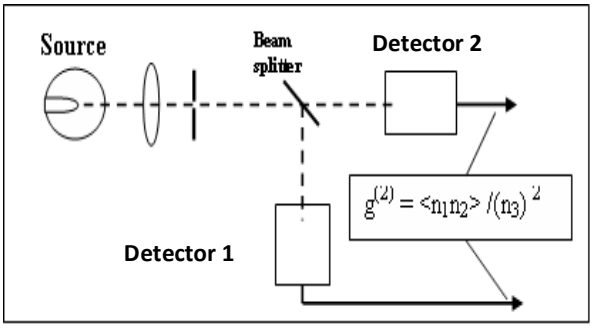


Fig. (4) : Arrangement of a Hanbury-Brown-Twiss interference [6]

The numbers of counts in each detector in a single run are not however in general the same. In quantum picture, each incident photon either passes the half silver mirror or is reflected from it. The average value $\langle n_1 n_2 \rangle$ of the product of counts in each single run, the correlation function, determines the extent to which coincident counts occur in the two detectors. The quantum analogue of the classical degree of second-order coherence is obtained by normalizing the second-order correlation function [6].

$$g^{(2)} = \langle n_1 n_2 \rangle / (n_3)^2 \qquad (6)$$

The second-order correlation function is used to characterize the intensity fluctuations properties of different light beams for single photon light beam $g^{(2)} = 0$. Table 2 summarizes the details of measurements obtained by HBT experiment.

Table (2): HBT experiment measurements. The columns show respectively the number of incident photons in HBT experiment (n),The possible number detected by the two phototubes (n_1, n_2), their mean (n_3), their Correlation ($\langle n_1 n_2 \rangle$), and the degree of second-order coherence $g^{(2)}$ [6].

N	n_1	n_2	n_3	$\langle n_1 n_2 \rangle$	$g^{(2)}$
	1	0			
			1/2	0	0
1	0	1			
	2	0			1/2
2	1	1	1	1/2	
	0	2			

Experimental work

Depending on many standard practical realizations to generate short pulses in the limits of few nanoseconds [7,8], an electronic circuit was designed to produce the 10 ns electrical pulses to meet the requirements needed to control the value of μ. Figure 5 shows the circuit that was implemented to control the value of μ.

Monostable type (SN74LS123) is positively edge triggered by TTL pulses, with frequency (f) equals to 1MHz. These pulses will produce a pulse ($\bar{Q}$) with a duration of about 100 ns with an amplitude between (3.5 to 4.5) V, TTL level. Then ($\bar{Q}$) will be used as an input to the

peripheral drivers for high-current switching at very high speeds, IC type (SN75451B). The output of (SN75451B) first circuit (Y_1) that intersects with ($\bar{Q}$) by the second circuit from the same IC to produce a pulse with duration ranges (12 to 20) ns.

Then this pulse is further treated by inductors (L) and capacitor (C) to increase the pulse amplitude in range of (8 to 20) V and decrease it's duration from 12 to 10 ns at the drain of CMOS-SST211. The inductor behaves as an open circuit at initial time closing of the switch, and the voltage across it decays exponentially. The time of decaying depends on the value of the inductor and the applied voltage across the inductor. The capacitor behaves in an opposite way of the inductor, i.e., as a short circuit at the initial time of closing the switch and the voltage across it will increase exponentially. The time of charging depends on the value of the capacitor and the applied voltage across it. At this point the pulse duration is reduced from τ_1 to τ_x as a result of the action for the LC network

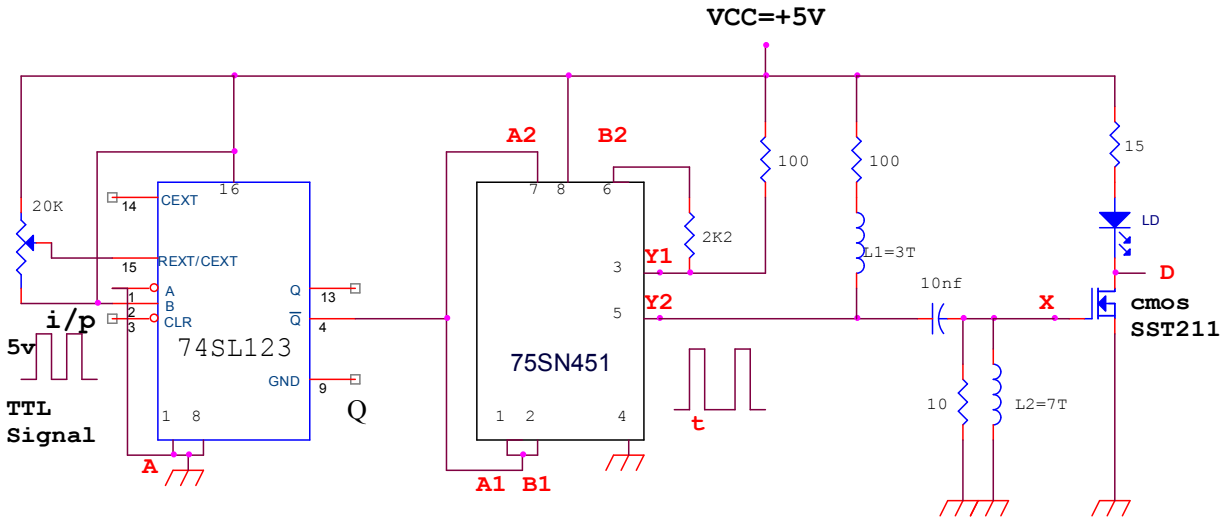


Fig. (5): The complete circuit diagram to generate 10 ns pulses.

Results and discussion

Figure 6 shows the output waveforms from the high speed switching peripheral device (Y_2) and the LC network (x) respectively.

The duration τ_x is slightly more than 10 ns, and it does not provide enough current to operate the LD.

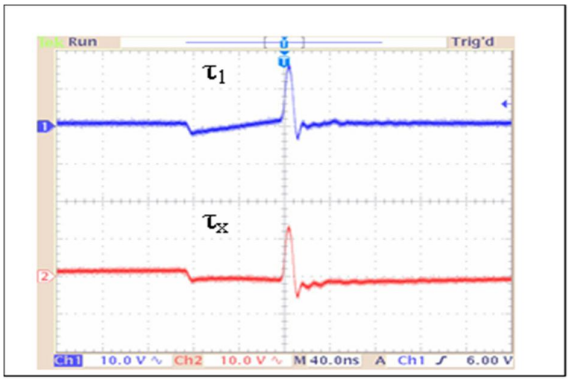


Fig. (6): Top: The output pulse at point $Y_2(\tau_1)$, Bottom: The output pulse at point $X(\tau_x)$.

Therefore, CMOS transistor (SST 211) was used to provide the sufficient current to operate the LD, also the CMOS transistor provides a high speed switching element for the circuit and by using the LC network on the gate of the CMOS transistor reducing the pulses to ranges about (6-8) ns. Figure 7 shows the final output pulses τ_x and τ at the CMOS drain. The circuit operates for repetition rate extending from 1 kHz to 10 MHz

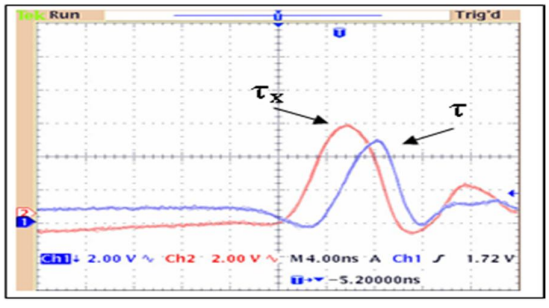


Fig. (7): The signal at point X with duration $\tau_x$and the signal at the drain of CMOS with duration τ (inverted τ).

Figure 8 shows the output signals at various points of the circuit.

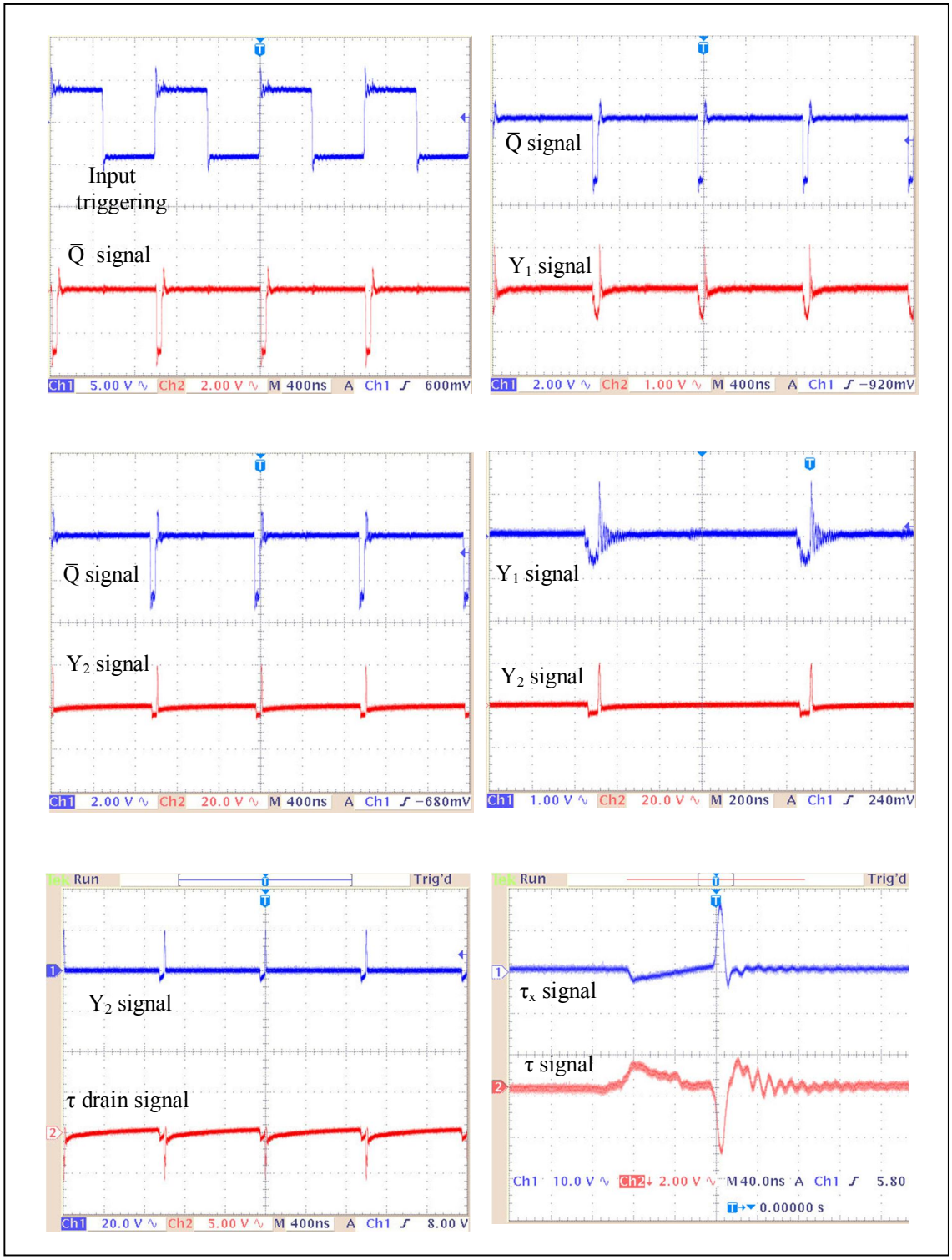


Fig. (8): Output waveforms of the circuit at various points of the circuit.

Tests and Measurements for controlling the value of μ

To obtain a laser pulse with average numbers of photons of $\mu \approx 0.1$ or less, many tests and measurements were done on the LD optical output pulse that was operated by the electrical pulse with a $\tau \approx 10$ ns.

These tests and measurements were directed into two directions. First, measuring the minimum average optical power for the LD to control the value of μ. Second, detection of these attenuated LD pulses by the single photon avalanche photodiodes (C30902S) working in the Geiger mode that are part of any quantum cryptography system.

These tests were carried out for two APD temperatures (15.9, -3) ^{o}C with various collections of optical filters and attenuators to attenuate the average optical power emitted by the LD as much as required to control the value of μ for various repetition rates. Average optical power for the LD operating by the electrical 10 ns pulse was recorded for various values of the repetition rate of the input triggering signal. The results obtained are listed in Table 3.

Table (3): Output optical average power for various input signal Repetition rates

f(kHz)	10	58	158	249	338	447	558	668	769	875	990	1000
P_{ave}(nW)	2	10	20	30	40	50	60	70	80	90	100	100

Various optical filters and attenuators (glass sheets) were used. Table 4 lists the values of μ obtained for various combinations of optical filters and attenuators at repetition rate of 10 kHz.

Table (4): Output optical average powerwith their corresponding mean photon number, μ. for 10 kHz

P_{ave} (W) at f =10 kHz, τ = 10 ns	**μ**
2×10^{-9}	653989
932×10^{-12}	304670.8
0.423×10^{-12}	13.827
14.8×10^{-15}	4.838
5.18×10^{-15}	1.693
0.267×10^{-15}	0.087

The value of μ was calculated as follows,
The average optical power of the laser diode is defined according to the following Equation [9]:

$$P_{ave} = N h\upsilon f \quad (7)$$

where,
P_{ave} is the average power in Watts,
N is number of photons per pulse,
f : is the repetition rate in Hertz.
The average optical power of a single photon is:

$$P_{single} = h\upsilon f \quad (8)$$

The number of photons per pulse is related to the duration of the pulse, and is calculated from,

$$N = \frac{P_{ave}}{P_{single}} \quad (9)$$

The single photon generation attenuation level,

$$\Upsilon = \frac{1}{N} = \frac{P_{single}}{P_{ave}} \quad (10)$$

In order to have 1 photon in every 10 optical pulses, i.e., μ =0.1, Equation 10 is written as,

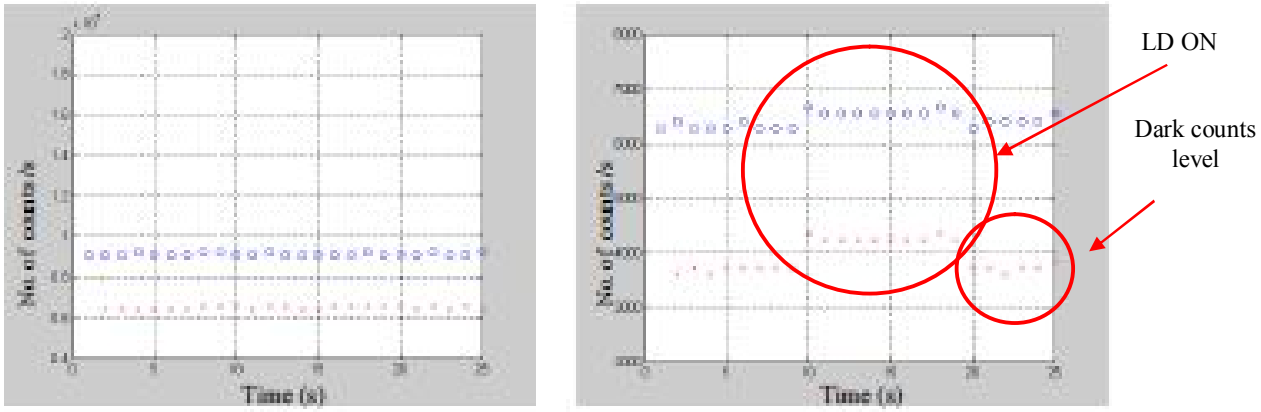
$$\Upsilon_{0.1} = \frac{0.1}{N} \quad (11)$$

This relation gives us the attenuation level required for μ =0.1

After generating these attenuated laser pulses by controlling the value of μ, tests were applied to detect these short attenuated pulses by the single photon avalanche photodiode used in any quantum cryptography system. Tests were made for maximum attenuation that was obtained with using collection of optical filters and attenuators. Figure 9 shows the APD counts for a laser diode emitting 2 nW average optical

power that was attenuated to 26.6 $\times 10^{-14}$ W. By applying Equation 2, μ is equal to 8.7 $\times$ 10^{-3}.

From Figure 9 it can be shown that when the laser diode is turned ON, number of APD counts increases with respect to the level of APD dark counts. Also as the APD temperature decreases the detection efficiency of the APD increases, i.e., increase in the APD counts.



a) T_{APD}=15.9 ^{o}C b)T_{APD}= -3 ^{o}C

Fig. (9): The effect of using attenuators and optical filters on the APD counts for 10MHz repetition rate, and μ = 8.7×10^{-3} .

Conclusions

The laser diode optical signal generated by driving the laser diode with these short pulses plus high attenuation can provide a very low value of μ = 8.7×10^{-3} (the minimum value of μ that can be obtained by our work). These short attenuated pulses will provide controlled weak coherent pulses needed in most quantum cryptography systems to enhance the security of these systems. Also weak coherent pulses can be used with decoy states (various values of μ). Decoy states helps in detecting Eavesdropping, increasing the transmission distance and increasing the rate of the key generation.

References

1. 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).
2. Wang, "A Solid-State Single Photon Source Based on Color Centers in Diamond" Dissertation at the Department of Physics at the Ludwig -Maximilians- University, Munich, June **08**, (2007).
3. Quyˆ enDinhXuˆan, Romain All´eaume, LiantuanXiao,a, Fran¸cois Treussart, Bernard Journet, and Jean-Fran¸coisRoch, "Intensity noise measurement of strongly attenuated laser diode pulses in the time domain".J. Appl. Phys. (35), **117**, (2006).
4. B. E. A. Saleh and M. C. Teich, "Fundamentals of Photonics" John Wiley and Sons, Inc. (1991).
5. H. Weier, "Experimental Quantum Cryptography", Diploma Dissertation, Technical University of Munich (2003).
6. R. Loudon, "Photon Bunching and Antibunching", reprinted from phys. Bull., 27 (1976).
7. R. J. Baker, "High voltage pulse generation using current mode second breakdown in a bipolar junction transistor", Rev. Sci. Instrum. **62**, pp.1031-1032 (1991).
8. O. Veledar, S. Danaher, J. I. H. Allen, P. O. Byrne, and L. F. Thompson, "Review and Development of Nanosecond Pulse Generation for Light Emitting Diodes", Journal of University of Applied Sciences, Mittweida. **9/10,** pp. 3-6 (2005).

9. J. Park, Y. Park, S. Lee, H. Shin, B.Bae and S. Moon, "Single-Photon Counting in the 1550-nm Wavelength Region for Quantum Cryptography", Journal of the Korean Physical Society, **49**, pp.111-114(2006).

توليد النبضات الضعيفة المتشاكهة لمنظومات التجفير الكمي

فـؤاد عـلي ياسـين [1] **شيـلان خسـرو توفـيق** [2] **احمـد اسماعـيل خليـل** [2] **فرح رياض عزيز** [2]

(1) مركز الحاسبة، جامعة بغداد ، بغداد ، العراق

(2) معهد الليزر للدراسات العليا ، جامعة بغداد ، بغداد ، العراق

الخلاصة هذا البحث هو محاولة للحصول على الأمنية المطلقة في اي استخدام لبروتوكول تجفير كمي من خلال بناء دائرة الكترونية فعالة للتقرب من متطلبات الفوتون المنفرد عن طريق السيطرة على معدل عدد الفوتونات المتولدة. و هذا يمكن تحقيقه عن طريق بناء دائرة قيادة تعطي نبضات قصيرة جداً تقارب (10 ns) الى الثنائي الليزري مع قدرة خرج (0.99 mW− 0.7) . وهذه النبضات القصيرة جداً تمكننا من الحصول على نبضات ضوئية خافتة جداً، والتي توهن للوصول الى معدل عدد الفوتونات مساوياً الى 0.08 أو أقل.