A Practical Quantum Cryptography Transmitter

Fouad Ali Yaseen
University of Baghdad
Computer center

ABSTRACT
The extend success of any communication system essentially depends on the strength of the secrecy of transporting the information between the partners. The classical cryptography for the wired and wireless communication systems can not withstand against the challenges of new technologies. So, it is necessary to invent a new method to encrypt the information. The solution is quantum cryptography in communication system. The absolute security can be achieve with quantum cryptography protocol via building an effective hardware for satisfying the single-photon source must requirement by controlling the value of mean photon number. This was approximately achieved in this work by building a driving circuit that provide very short pulses, less than 10 ns for Laser Diode with output maximum power of 0.99 mW and wavelength 650 nm. These short pulses enable getting faint laser pulses that were further attenuated to reach mean photon number equal to 0.08 or less.

Keywords
Single Photon Source, Quantum Cryptography (QC), Quantum Key Distribution (QKD).

1. INTRODUCTION
The quantum cryptography is provable unconditional security between communication parties is, according to the uncertainty principle in quantum mechanics, the polarization of a photon in the rectilinear and diagonal basis, can never be measured precisely and simultaneously. 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 photonic 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]. Attenuated laser pulses are commonly used instead of "real" single photons source. In laser pulses the mean number of the photons follows the Poissonian distribution, the laser pulse contains probability of non-vanishing two or more photons within a single 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. An eavesdropper can share almost all the information without being detected that for a quantum channel with high loss it is possible for. Therefore the implementations of quantum cryptography (QC) 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 is an open door to information leakage towards an eavesdropper. Weak Coherent Pulses (WCPs) are used instead of pure single-photon pulses to guarantee unconditional security for practical setups [3]. 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. The quantum transmitter consists of two parts electronic and optical. Electronic part is responsible of generating electrical pulses which drive the laser diode (LD). LD is responsible of generating optical pulses, these pulses involve the photons. Our work is focused on building an electronic circuit to generate pulses less than 10 ns to get the average photon number per pulse ($\mu < 1$). Authors In [4] present performance tests of a new design based on polarization encoding of attenuated, coherent light pulses. To improve security of long-distance QKD, refined protocols like "differential phase-shift" QKD and "decoy-state" QKD, have been proposed in [3]. The standard BB84 protocol has been implemented in [5] with decoy states16–19 with photon fluxes of 0.5, 0.1, and 0.0002 photons per pulse. They determined the secure bit rate for each user individually by estimating single-photon parameters from decoy states. Authors in [6] got experimental results show that the proposed transmitter is suitable for implementation of the BB84, coherent one-way (COW) and differential phase shift (DPS) protocols with stable and low quantum bit error rate. This could become a useful component in network QKD, where multi-protocol capability is highly desirable.

2. 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 [7],

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

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

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

The probability distribution expression p(*n*) can be derived according to registrations of photons are statistically independent, the result is Poisson distribution[7].

$$P(n) = (\mu^n / n!) \cdot e^{-\mu}, \quad n= 0, 1, 2, \ldots \quad (3)$$

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, $\mathbf{p= \mu / N}$, 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[7],

$$P(n) = [N!/\{n!(N-n)!\}]\, p^n (1-p)^{N-n}$$
$$= [N!/\{n!(N-n)!\}]\, (\mu/N)^n \{1-(\mu/N)\}^{N-n} \quad (4)$$

If $N \to \infty$, $[N!/(N-n)!N^n] \to 1$, and $[1-(\mu/N)]^{N-n} \to e^{-\mu}$, so that Equation 3 is obtained [7].

By applying Equation 3 for $\mu = 0.1$ and $\mu = 0.2$ with various values of n, $p(n, \mu)$ values are listed in table 1,

Table 1: The probability of photon number with μ=0.1 and 0.2

μ	0.1	0.2
P(0, μ)	0.9048	0.8187
P(1, μ)	0.09	0.1637
P(2, μ)	$45*10^{-4}$	$164*10^{-4}$
P(3, μ)	$15*10^{-5}$	$11*10^{-4}$
P(4, μ)	$377*10^{-8}$	$55*10^{-6}$
P(5, μ)	$754*10^{-10}$	$22*10^{-7}$

3. CALCULATING AVERAGE NUMBERS OF PHOTONS

To get a laser pulse with average numbers of photons of μ less than 0.1, the LD was driven by the electrical pulse with a $\tau \leq 10$ ns that generated by our circuit. The optical output pulse measured, the measurements steered into tow paths. First, calculating μ from average optical power which emitted from LD. Second, sapping the LD optical pulses and detecting these pulses by single photon avalanche photodiode (C30902S) operating in Geiger mode. These operations were implemented at (-3 °C) with several optical filters and attenuators for various input triggering frequencies. The measurements results are listed in table 2.

Table 2: Output optical average power for various input triggering frequencies

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

Various optical filters and attenuators were used to attenuate the average optical power emitted by the LD as much as required to control the value of μ .

Table 3 lists the values of μ obtained for various combinations of optical filters and attenuators at repetition rate of 10 kHz and electrical pulse 10 ns.

Table 3: Output optical average power with their corresponding mean photon number, μ. for 10 kHz

P_{ave} at f=10 kHz, τ = 10 ns	**μ**
2 nW	653989
932 pW	304670.8
0.423 pW	13.827
14.8 fW	4.838
5.18 fW	1.693
0.267 fW	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 (5):

$$P_{ave} = Nh\upsilon f \quad (5)$$

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:

$$P_{single} = h\upsilon f \quad (6)$$

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

$$N = \frac{P_{ave}}{P_{single}} \quad (7)$$

The single photon generation attenuation level,

$$\Upsilon = \frac{1}{N} = \frac{P_{single}}{P_{ave}} \quad (8)$$

In order to have 1 photon in every 10 optical pulses, i.e., μ =0.1, Equation (9) is written as:

$$\Upsilon_{0.1} = \frac{0.1}{N} \quad (9)$$

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 attenuated pulses by the single photon avalanche photodiode of QC system. Tests were made for maximum attenuation that was obtained with using collection of optical filters and attenuators. Figure 1 shows the APD counts for a laser diode emitting 2 nW average optical power that was attenuated to 26.6×10^{-14} W. By applying equation 2, the value of μ is 8.7×10^{-3}.

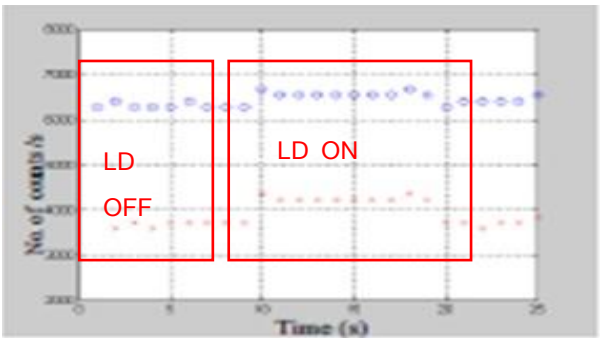

Figure 1: Detecting the LD optical output By two APDs for 10 MHz repetition rate.

4. EXPERIMENTAL WORK

An electronic circuit was designed to produce the 10 ns electrical pulses to meet the requirements needed to control the value of μ .

Figure 2 shows the block diagram of the circuit that was implemented to control the value of μ .

The operation of the circuit is summarized as follows:
The monostable is positively edge triggered by TTL pulses, with frequency range (f) about (1kHz -10 MHz).

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. The output of high-current switching 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 The resistor, inductor and capacitor (RLC) network, to increase the pulse amplitude in range of (8 to 20) V and decrease it's duration from 12 to 10 ns at the gate of CMOS. 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 Y_2 to τ as a result of the action for the RLC network. Then CMOS driver drives the LD by very narrow electrical pulses τ_x with FWHM pulse duration about 5 ns. Then LD emits a faint optical pulses which mimic the single photon source.

5. RESULTS AND DISCUSSION

Figure 3 shows the output waveforms from the high speed switching peripheral device (Y_2) and the RLC network inverted (τ) respectively and illustrates FWHM for (τ) signal.The duration Y_2 is slightly more than 10 ns, and it does not provide enough current to operate the LD.

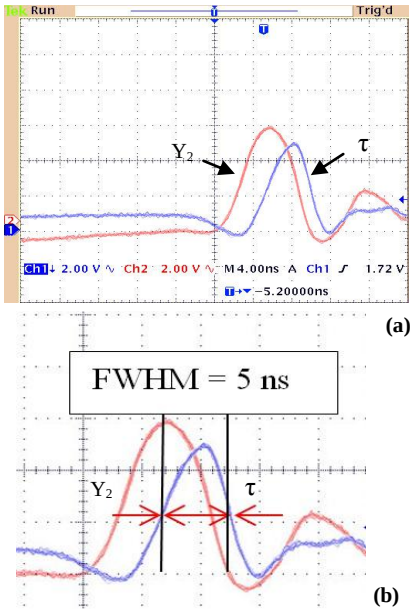

Figure 3: (a) The signals Y_2 and τ, (b) FWHM of τ

Therefore, CMOS transistor 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 RLC network on the gate of the CMOS transistor reducing the pulses to ranges about (5-8) ns.

Figure 4 shows the final output pulses τ and τ_x at the CMOS gate and drain respectively.

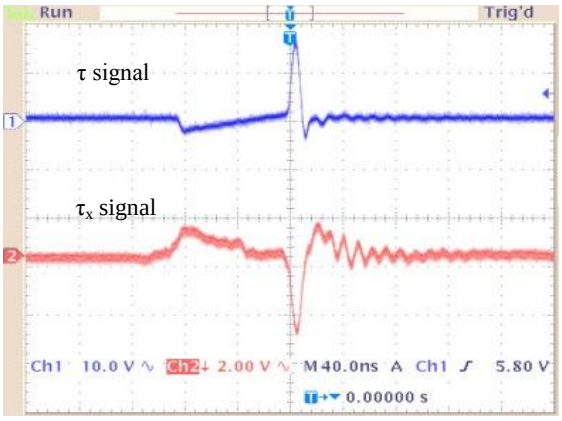

Figure 4: Output waveforms at gate and drain of the CMOS of the circuit.

6. CONCLUSIONS

The laser diode optical signal generated by driving the laser diode with these short pulses can be detected by single photon avalanche photodiodes for a very low value of $\mu = 8.7\times10^{-3}$ that represents the minimum value of μ which can be obtained by this work. These short pulses will provide 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). Besides weak coherent pulses help in studying eavesdropping strategies.

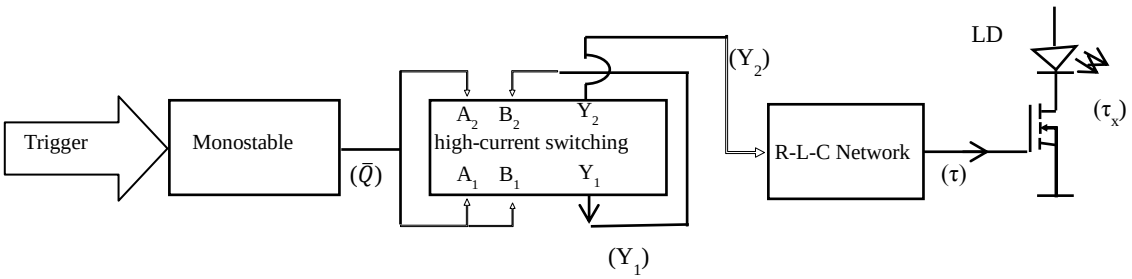

Figure 2: shows the block diagram of the practical circuit.

7. 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] C. Wang, "A Solid-State Single Photon Source Based on Color Centers in Diamond" Dissertation at the Department of Physics at the Ludwig-Maximilians-Universit¨atM¨unchen, M¨unchen, June 08, 2007

[3] Quyˆ enDinhXuˆan, RomainAll´eaume, LiantuanXiao,a, Fran¸coisTreussart, 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] S. Chiangga, P. Zarda, T. Jennewein, H. Weinfurter, "Towards practical quantum cryptography" Appl. Phys. B 69, 389–393 1999.

[5] Bernd Fr¨ohlich, James F Dynes, and et al. "A quantum access network" , arXiv:1309.6431v1 [quant-ph], 25 Sep 2013.

[6] Boris Korzh, Nino Walenta, and et al, "A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator", Optical Society of America, 2013.

[7] B. E. A. Saleh and M. C. Teich, "Fundamentals of Photonics" , John Wiley and Sons, Inc. 1991.