Iraqi J. Laser, Issue (1), Vol.18, pp.31-42 (2019)

IRAQI JOURNAL OF LASER

Generation of True Random TTL Signals for Quantum Key-Distribution Systems Based on True Random Binary Sequences

Salwa M. Salih [(1)] **Shelan K. Tawfeeq** [(2)] and **Ahmed I. Khaleel** [(3)]

(1) Osouledeen University College, Baghdad, Iraq
(2, 3) Institute of laser for postgraduate studies, University of Baghdad, Baghdad, Iraq

(Received 1 November 2018; accepted 3 December 2018)

Abstract: A true random TTL pulse generator was implemented and investigated for quantum key distribution systems. The random TTL signals are generated by low cost components available in the local markets. The TTL signals are obtained by using true random binary sequences based on registering photon arrival time difference registered in coincidence windows between two single – photon detectors. The true random TTL pulse generator performance was tested by using time to digital converters which gives accurate readings for photon arrival time. The proposed true random pulse TTL generator can be used in any quantum -key distribution system for random operation of the transmitters for these systems.

K**ey words:** true random numbers, time to digital converter

Introduction

Quantum Key Distribution (QKD) is the art of sharing secret keys between two remote parties Alice and Bob, unconditional security of which is based on the fundamental laws of quantum mechanics. It is a perfect solution to distribute a secret key between two remote parties with absolute security. It is also one of the first practical applications that it based on single photons. In the early days of this technology, experimental progress was not noticeable , but it quickly became more and more practical, with major improvements being developed .One of the key features for QKD security is the need of Random Number Generators (RNGs) that the parties use to choose the basis in which they measure the transmitted bit. All QKD protocols depend on the ability to generate true random numbers. In the BB84 protocol, for example, Alice randomly creates a classical bit string to be transmitted, and for each bit she also randomly selects between two distinct maximally overlapped bases for qubit encoding. Bob, randomly and independently from Alice, also chooses for each incoming qubit the same two bases. Also, random change in analyzers orientation in entanglement quantum key distribution for Bell's inequality tests is essential. In order to perform truly random and independent choices, a hardware-based true QRNG must be used by both Alice and Bob, as any software RNG actually generates a pseudo-random sequence [1-3]. It can be easily proved that the measurement outcomes will become unsafe if the input random numbers are controlled or known by the eavesdropper Eve. Two important elements are essential in practical QKD system, the random preparation and measurement of quantum states. If these procedures are imperfect, which can be perceived as a kind of incomplete randomness, the deviation may be used to perform quantum attacking [3].

In this paper, some of our previous works for true RNGs are reviewed followed by an experimental setup which consists of a true random TTL signal generator corresponding to true random sequences obtained from our

previous work [4].The true random sequence is based on registering photon arrival time difference registered in a coincidence window between two single – photon detectors.

True random number generators

Many methods are used for random number generation. Mainly these methods are based on either simple mathematical techniques which give pseudo random numbers or physical sources that give truly random numbers. Either types of random numbers, pseudo or true, depends on the application. Recent applications of quantum cryptography where unconditional security is required, can not depend on pseudo random numbers because they are deterministic and periodic and are not sufficient for these applications. To achieve unconditional security which is based on laws of quantum physics true random numbers are needed. True random numbers are essential in these applications that use quantum cryptography for random bases orientation change [5]. Many methods were applied for generation of true random numbers ranging from simple setups to more complicated methods. A simple setup of random number generator was proposed based on the shot-noise fluctuations in a p-i-n photodiode. These fluctuations that are defined as shot noise are based on a stationary random process whose statistical properties reflect Poisson statistics associated with photon streams. It has its origin in the quantum nature of light and it is related to vacuum fluctuations. Two photodiodes were used and their shot noise fluctuations were subtracted. The difference was applied to a comparator to obtain the random sequence. The circuit block diagram is shown in Figure (1). The binary sequence obtained from this setup was tested for randomness by the ENT program that computes the entropy, chi square, arithmetic mean, Monte Carlo estimation of π and the serial correlation coefficient [5].

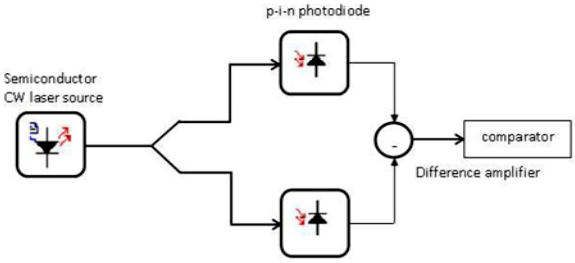

Fig.(1): The circuit block diagram to generate random numbers based on shot-noise fluctuations in a p-i-n photodiode [5]

Figure (2) shows the schematic diagram of physical random number generator based on dark pulses thermally generated by single-photon avalanche photodiodes working in the Geiger mode. This proposed true random number generator produced a random sequence with approximately 50% 0s and 50% 1s. This source of true random sequence can be considered as an acceptable source for randomness in quantum cryptography systems [6]. Also the binary sequence obtained passed the ENT test for randomness.

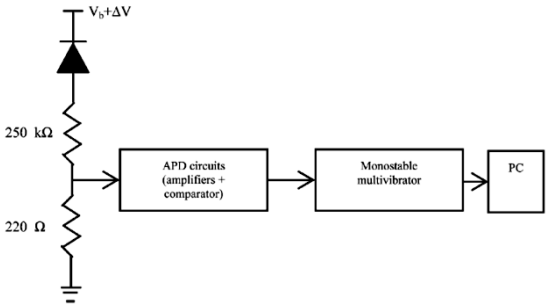

Fig.(2): Schematic diagram for generating random numbers based of dark counts of single-photon avalanche photodiodes [6]

The random arrival times of photons on a photo detector can be used as the quantum random variable. The interval between successive photons from a light source with Poisson statistics is divided into individual time bins. The time interval between subsequent photon detections is exponentially distributed. The waiting-time is of a Poisson process. The time intervals can then be used to create several random bits per detection event. The arrival time of the photons is illustrated in Figure (3) [7].

Fig.(3): The random time of arrival of consecutive photons of attenuated laser source [7]

True random number generators based on photon arrival times have an output waiting-time distribution of the form of e^{-Rt}, where R is the photon rate of single-photon detector and t is the time until the next photon is detected [8].
The rate of incoming detections and the time resolution with which they can be measured by a time to digital converter (TDC) affect the amount of entropy that can be extracted [8]. A high rate of detection results in reduced entropy per photon detection, but it increases the overall bit rate due to more frequent photon detections. However, the increase in detections per second is limited asymptotically by the dead time of the single-photon detector (T_{dead}), i.e., the time after a detection during which the detector will not register incoming photons. The effective photon rate, R_{photon}, is the rate at which photons are registered. This means it represents the random number generation rate [5,8]

$$R_{photon} = R/(1 + R \times T_{dead}) \quad (1)$$

Figure (4) shows the experimental setup for the true random number generator based on the difference in photon arrival times in the coincidence window between two single-photon counting modules.

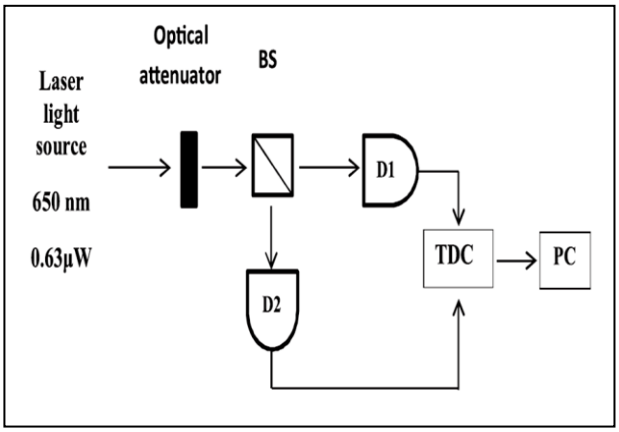

Fig. (4): The experimental setup of random number generation based on the photon arrival time in a coincidence window between two single photon counting modules, BS: beam splitter, D1: single-photon counting module1, D2: single-photon counting module 2, TDC: time to digital converter, PC: personal computer [4].

The random binary sequences obtained from this setup passed the NIST (National Institute of Standards and Technology) statistical test suite for randomness [4**].** One of these files was used in the current experiment to provide the true random sequence used to generate the TTL signals needed in QKD experiments. NIST statistical test suite has 15 statistical tests that all together search for different types of non-randomness that might exist in long binary sequences generated by any hardware or software. These tests can be applied to a sequence as an attempt to compare the sequence to a truly random sequence [9].
The binary true random sequences obtained were saved in files. One of these files was used in the current experiment to provide the true random sequence used to generate the TTL signals needed in QKD experiments such as BB84 Protocol and Measurement Device Independent -QKD Protocol (MDI-QKD).

QKD Protocols

The BB84 protocol, named after its inventors Bennett and Brassard, is the first and the most common QKD protocol. This protocol is a prepare-and-measure protocol, in which, the sender (Alice) performs the encoding by preparing the quantum states, and the receiver (Bob) measures them.
In this protocol, photons are prepared by Alice with polarization randomly chosen from one of these four states: horizontal (0º), vertical (90º), diagonal (45º), anti-diagonal (135º). Rectilinear (0º, 90º), R, and diagonal (45º, 135º), D, basis are randomly chosen by Bob to measure each photon's polarization state. The schematic setup for this protocol is shown in Figure (5).

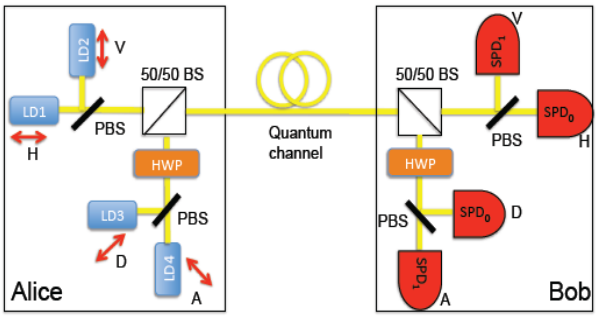

Fig.(5): Schematic of a QKD system implementing the BB84 protocol. LD: laser diode; BS: beam splitter; SPD: single-photon detector; HWP: half wave plate [10].

The steps of the protocol are shown in Table (1)

Table (1): BB84 protocol step

Alice's random bits	1	0	0	1	0	0	1	1	0
Alice's sending basis	R	D	R	D	D	D	D	D	R
Alice's photon polarization	↕	↗	↔	↘	↗	↗	↘	↘	↔
Bob's receiving basis	D	R	R	D	D	R	R	D	R
Bob's key bits	0		0		0	1	1	1	
Bob checks the bases with Alice			Ok		Ok			Ok	
Bob and Alice check some key bits randomly					Ok				
Sifted key			0					1	

A lot of work has been done to build loophole-free QKD systems with practical devices. Building better models was required to understand all the imperfections in a QKD detection system but it is almost impossible to guarantee that all the loopholes have been fixed [11]. MDI-QKD protocol was proposed in 2012 by Lo, Curty, and Qi [12]. Figure (6) shows the basic setup for MDI-QKD system. This protocol gave a promising solution to the security problem of practical QKD systems. Compared to other protocols, MDI-QKD removes all (existing and those yet-to-be-discovered) security loopholes in the detectors. MDI-QKD still requires trusted sources. In MDI-QKD protocol, Alice and Bob prepare phase randomized weak coherent pulses (WCPs) in a different polarization states, 90º, 0º, 45º, -45º which is selected, independently and at random for each signal. Inside the measurement device, signals from Alice and Bob interfere at a 50:50 beam splitter (BS) that has on each end a polarizing beam splitter (PBS) projecting the input photons into either horizontal (H) or vertical (V) polarization states. Four single-photon detectors are employed to detect the photons and the detection results are publicly announced [12].

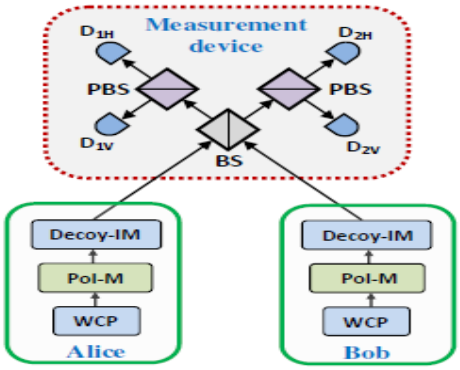

Fig.(6) : the basic setup for MDI-QKD setup. WCP: weak coherent pulses, Pol-M: polarization modulator, IM:intensity modulator, PBS: polarizing beam splitter, D: single-photon detector [12]

Figure (7) shows an experimental setup of the first experimental demonstration of polarization encoding MDI-QKD over 10 km of optical fibers. All the modulators, phase modulators (PMs) , acousto-optic modulators (AOMs) , and polarization modulators (Pol-Ms) are independently driven by random number generators (function generators with prestored random numbers generated by a quantum random number generator . An electrical delay generator (DG) located in Charlie's setup synchronizes all the RNGs and the electrical pulse generators (PGs) driving the IMs [11].

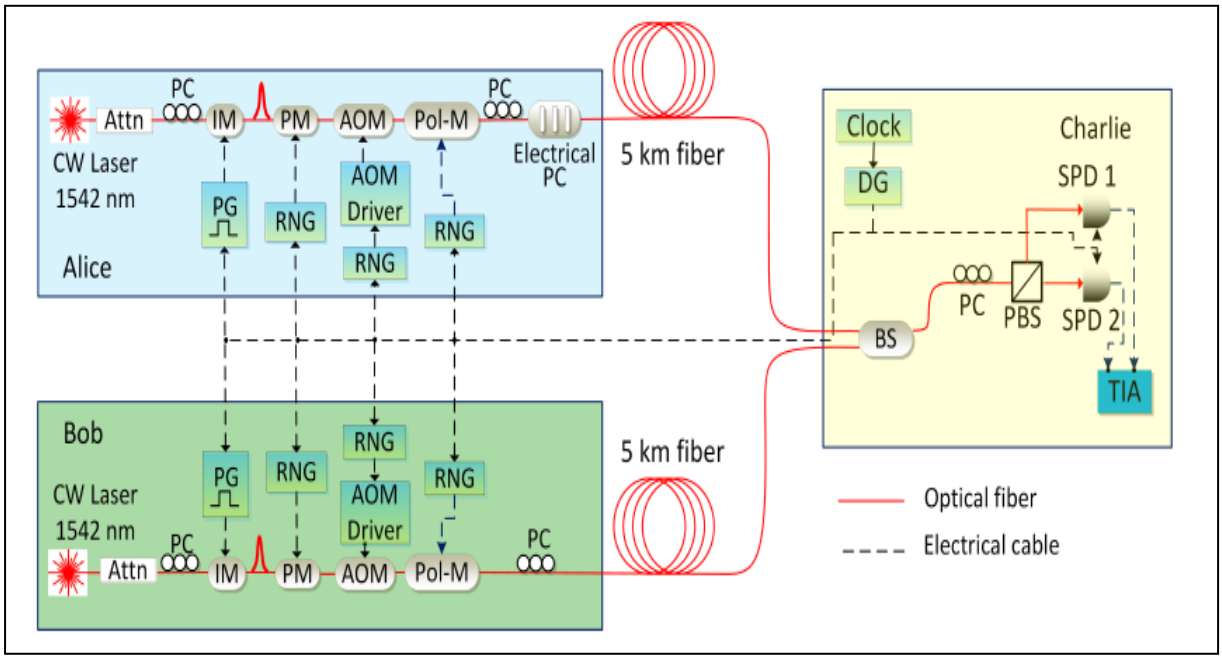

Fig.(7): Experimental setup of polarization encoding MDI-QKD. PG: pulse generator, RNG: random number generator, AOM: acousto optic modulator, SPD:single-photon detector [11].

The setup shown in Figure (8) is for a MDI-QKD system over 200 km [13]. The phases of the directly modulated pulse trains are intrinsically random to make guarantee that the system is immune to the unambiguous state-discrimination attack. Alice (Bob) uses an amplitude modulator (AM) to randomly modulate the laser into three different intensities. All the modulators, including the AMs and the PM, are controlled by the random numbers of Alice and Bob independently [13].

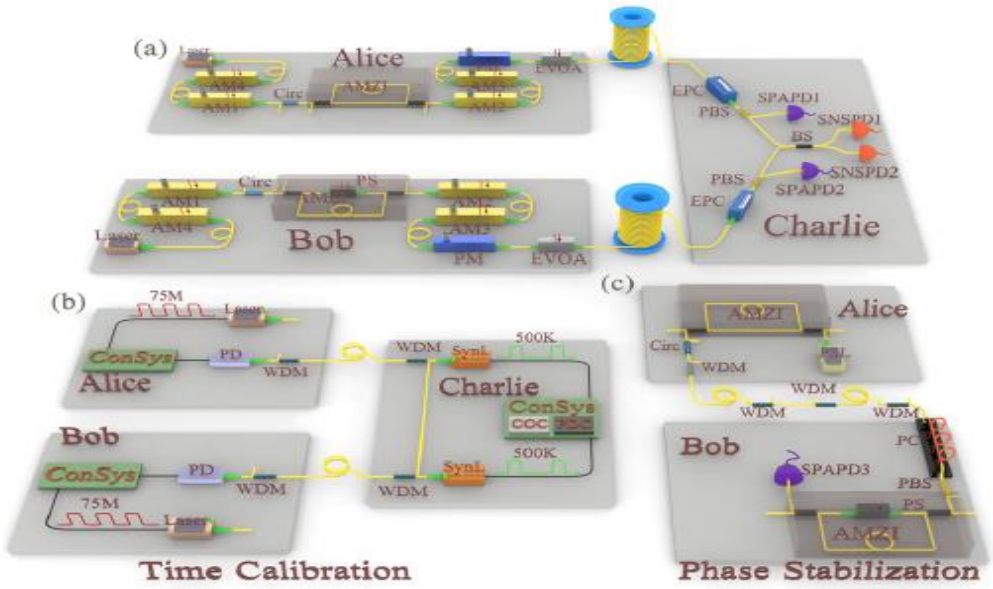

Fig.(8): Schematic layout of our MDI- QKD setup. PBS:polarizing beam splitter, PD: photodetector, SPAPD: superconducting nanowire single-photon, AMZI: asymmetrical Mach-Zehnder interferometer, PM:phase modulator, PC: polarization controller, PS: phase shifter, Circ: circulator, ConSys: control system, COC: crystal oscillator circuit, PDC: programmable delay chip, EPC : electric polarization controller [13].

Experimental setup and results

The experimental setup for generating true random TTL signals to control the operation of laser sources randomly at the transmitters of quantum cryptography systems was designed and implemented. The true random TTL signals generator was investigated by time to digital converter TDC from IDquantique (id800) which composes of 8-channel time-to-digital converter, coincidence counter, and time interval analyzer.
The basic building block for this generator is the Arduino Uno REV3 which is a microcontroller board relied on ATmega328p. It has the properties listed in the Table (2). It was programmed using a simplified C++ language in a processing-based Integrated Development Environment (IDE).

Table (2): Arduino Uno technical specifications

Operation voltage	5 V
Clock speed	16 MHz
Digital I/O pins	14 (of which 6 provide PWM output)
Flash memory	32 KB
SRAM	2 KB
EEPROM	1 KB

The Nanosecond Pulsed Lasers are from THORLABS, NLP64B were used in this setup. The operating wavelength is 640 nm, maximum average output power is equal to 20 mW and pulse width (FWHM) ranges from 5 ns to 39 ns. The laser output power was equal to 2 µW and operated at a repetition rate of 10 kHz.
Two SPCMs from the PDM series with serial numbers (00952) and (00947) were used for detecting the optical pulses. The SPCM generates a TTL signal per detected photon of 3.5 V and output pulse duration of 20 ns with a photon detection efficiency of approximately 38% at a wavelength of 640 nm. The dark count rate is equal to 71 c/s. The SPCM is thermoelectrically cooled.
Two types of random sequences were generated and tested for the random operation of the LDs, pseudo random sequences and true random sequences. Random TTL signals are generated according to pseudo random binary sequences and true random sequences that are stored in a text file. This was done by connecting a SD Card shield with Arduino UNO and each character (represented by 0 or 1) was read from the text file by a program. A TTL signal was generated representing 0s and 1s.
The program that controls Arduino UNOs consists of two parts. The first parts was to for reading the 240 characters, each character is represented by 8 bits (1 byte), stored in the SD card and were compressed into an array of 30 bytes, each byte consists of 0s and 1s. The second part was for generating TTL signal representing these 30 bytes (0s and 1s) whenever an external signal triggers the Arduino UNO. Figure (9) shows the flowchart of Arduino UNO's programming.

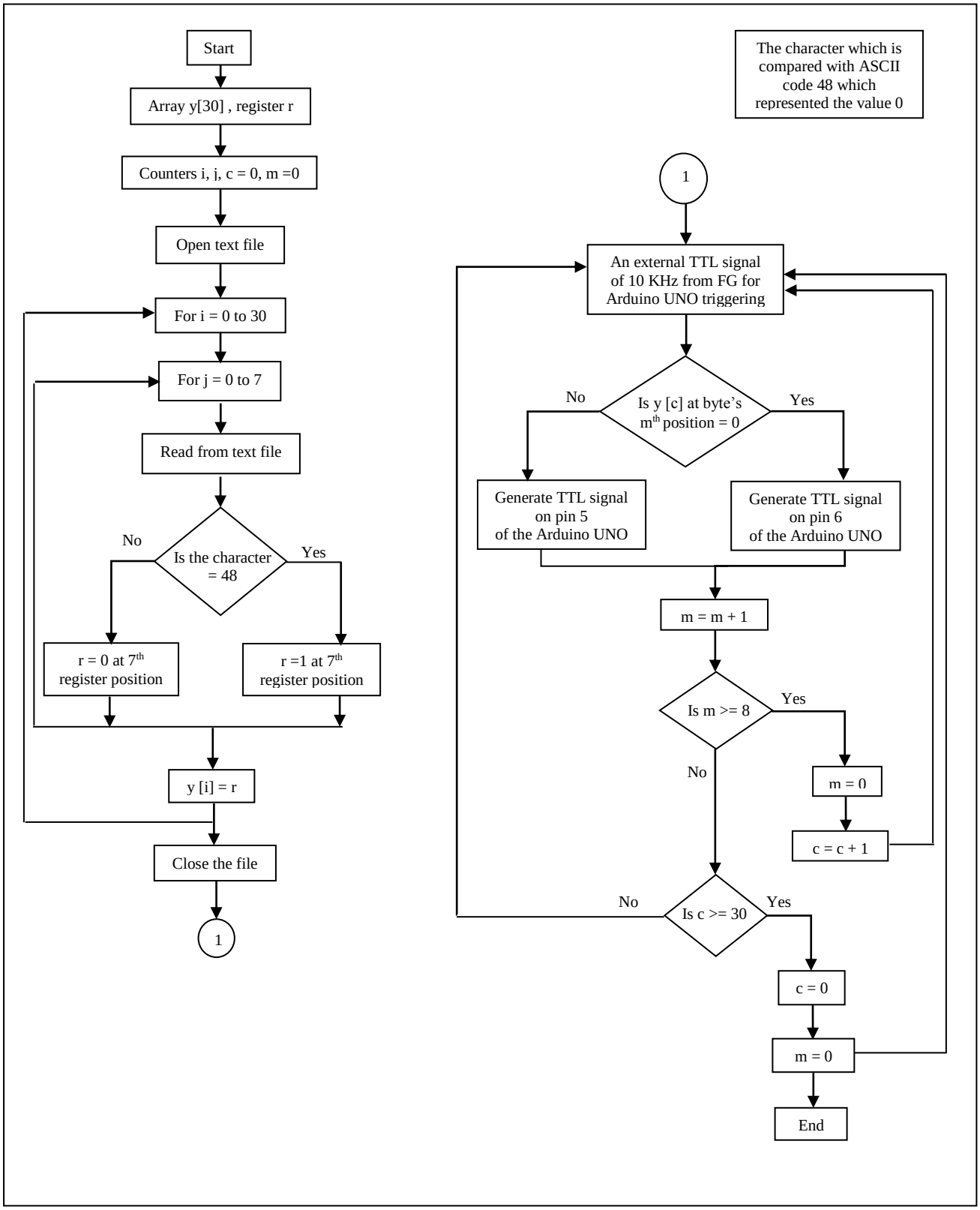

Fig. (9): Flowchart of Arduino UNO's programming

Figure (5) shows the setup used to control random operation of two laser diodes (LDs). A function generator was used to trigger the LDs with TTL signal of 10 KHz.The LD output pulse width is equal to 5 ns.

The experimental setup used for controlling the LDs' operation is shown in Figure (10). One Arduino UNO is used to randomly control the operation of the two LDs with different percentages of 0s and 1s. The operation of the LDs was investigated by TDC working as a counter and time tag analyzer.

When the TDC works as a counter, it counts the number of detected photons by SPCMs.

When the TDC works as a time tag analyzer, it records the value of the clock at the time of an event and on which channel it occurred.

Each detected photon corresponds to a pulse emitted by the corresponding LD that is operated by a TTL signal generated by the Arduino UNO. The setup is arranged in a manner that the 0s operate LD1 and 1s operate LD2.

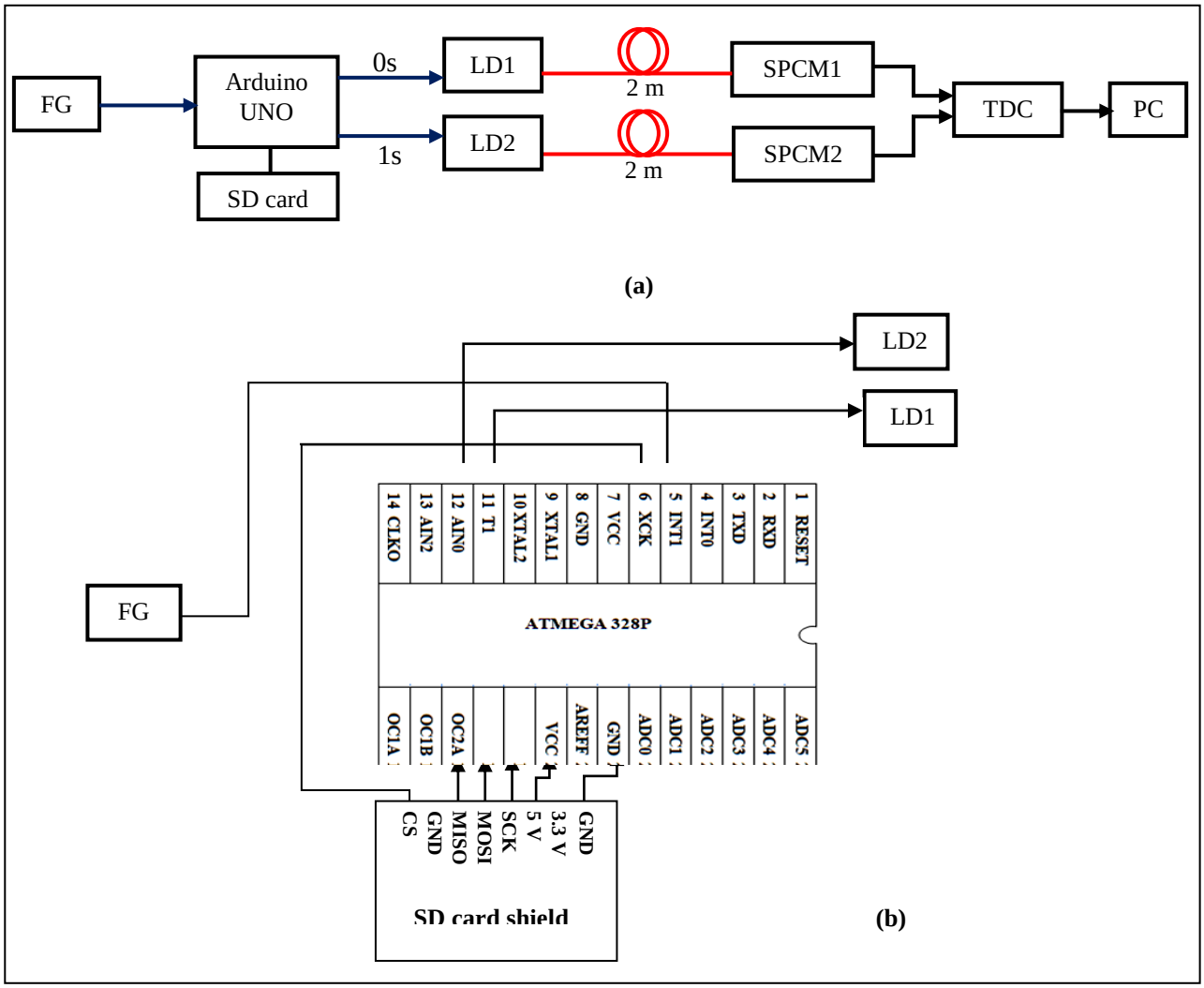

Fig.(10):(a) Experimental setup used to control random operation of two**,(b):** Arduino UNO connctions

A- Generation of pseudo random sequences:

Random electrical signals were generated based on pseudo random sequences saved in a file with known percentages of (0s) and (1s). Different files of different percentages of 0s and 1s were tested for the setup shown in Figure (10). The 30 bytes in these files included the same repeated patterns of 0s and 1s.These files were used to check the random operation of LDs with an oscilloscope and TDC. Figure (11) shows different signals and counts for different percentages of 0s and 1s. It is clear from the results that the TDC gives approximately the same number of counts that corresponds to the

percentages of 0s and 1s (62% and 38%, 25% and 75% and 50% for both) that were generated by the Arduino UNO which gives TTL signals to operate the LDs. The total number of counts appearing in the TDC results is approximately equal to 10000 c/s which corresponds to 10 KHz repetition rate of the function generator. The total number of counts exceeds 10000 (the repetition rate of the FG=10 KHz) because of the dark counts. These results show that the LDs are responding to the TTL random signals.

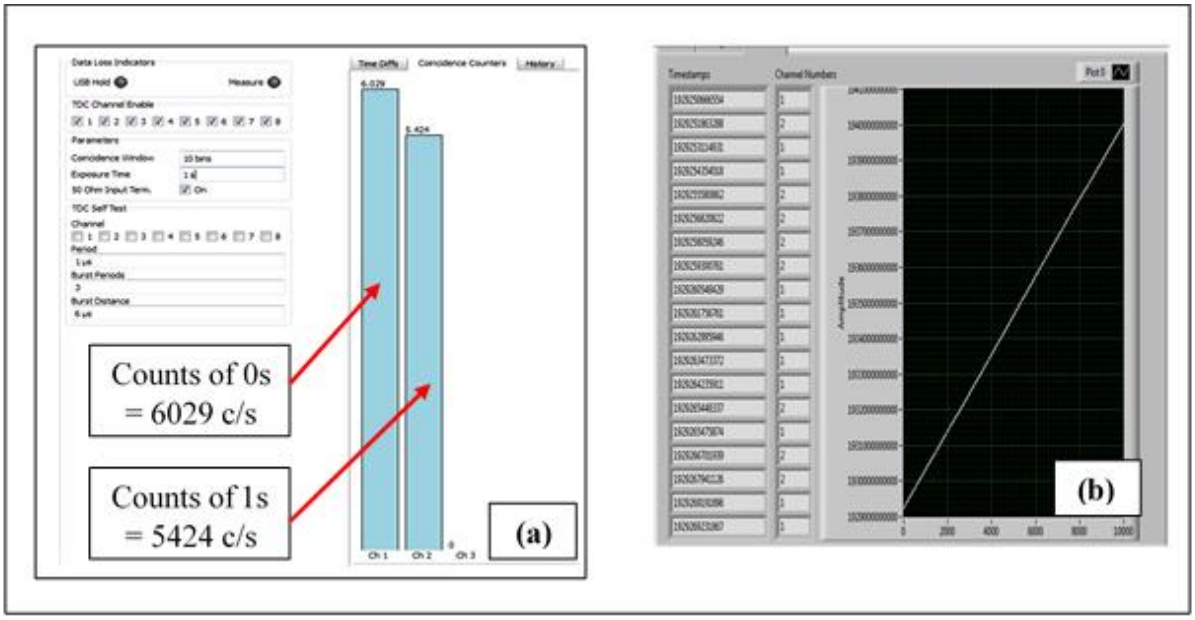

Fig.(11): A 10000 pseudo random sequences recorded at ch1 and ch2 of (a, c, e): TDC, (a) 62% 0s and 38% 1s, (c) 25%0s and 75% 1s, (e) 50% 0s and 1s, (b, d ,f):Oscilloscope

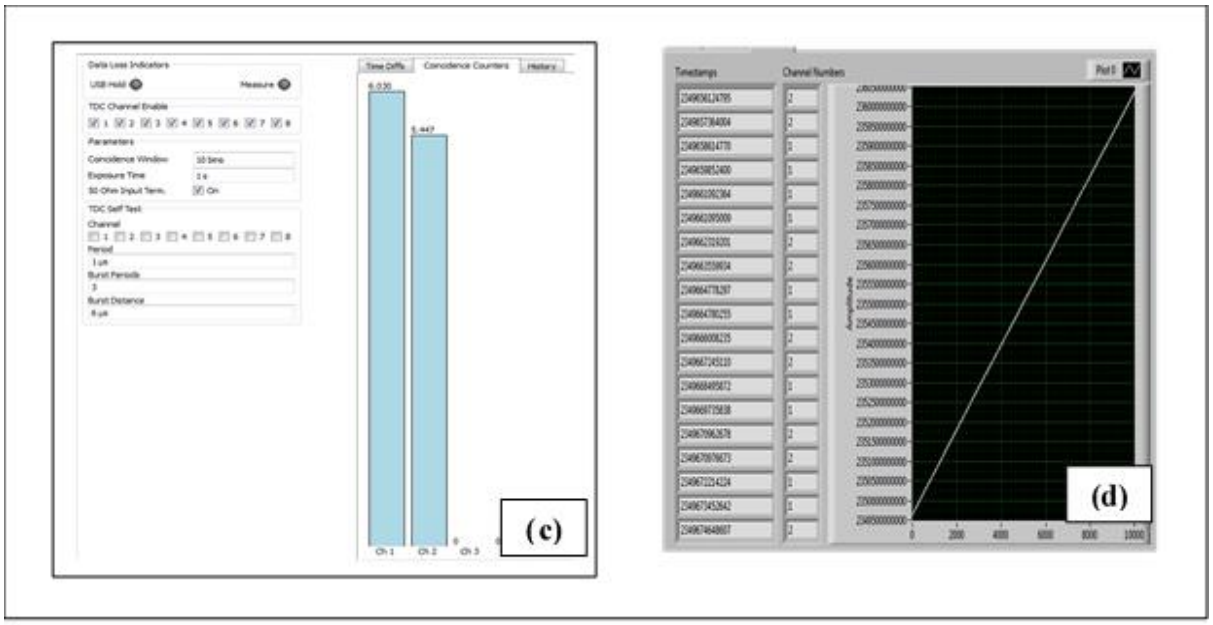

Fig.(11): Continued

B- Generation of true random TTL signals

True random binary sequences based on registering photon arrival time difference registered in coincidence windows between two SPCMs [4] stored in a text file in SD card were used to generate the true random TTL signals.

Figure (12) shows the true random TTL signals generated by the Arduino UNO. The TTL signals are randomly distributed and will operate the LDs randomly.

Figure (13) shows the results obtained by TDC counters and time tags. As far as the sequence is a true random sequence, it should have approximately 50% 0s and 50% 1s. This is clear in the number of counts registered by the TDC, Figure (13-a, c). It is clear also that the number of counts are different in both Figures (8-a, c) each time the system operates, but the percentage of approximately 50% 0s and 50% 1s is always recorded.

Figure (8-b, d) shows the time tags for the photon arrival times detected by the SPCMs. It is clear also that recording channels 1 and 2 (corresponding to SPCM1 and SPCM2 respectively) are random and is different for different screen shots of the TDC.

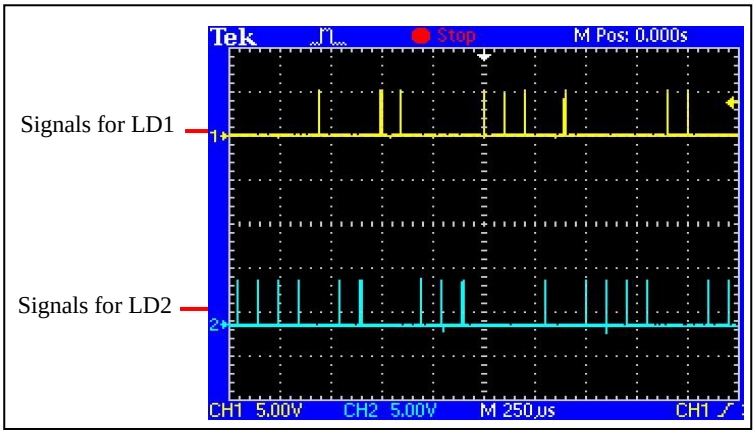

Fig.(12): A 10000 true random sequences recorded at ch1 and ch2 of Oscilloscope

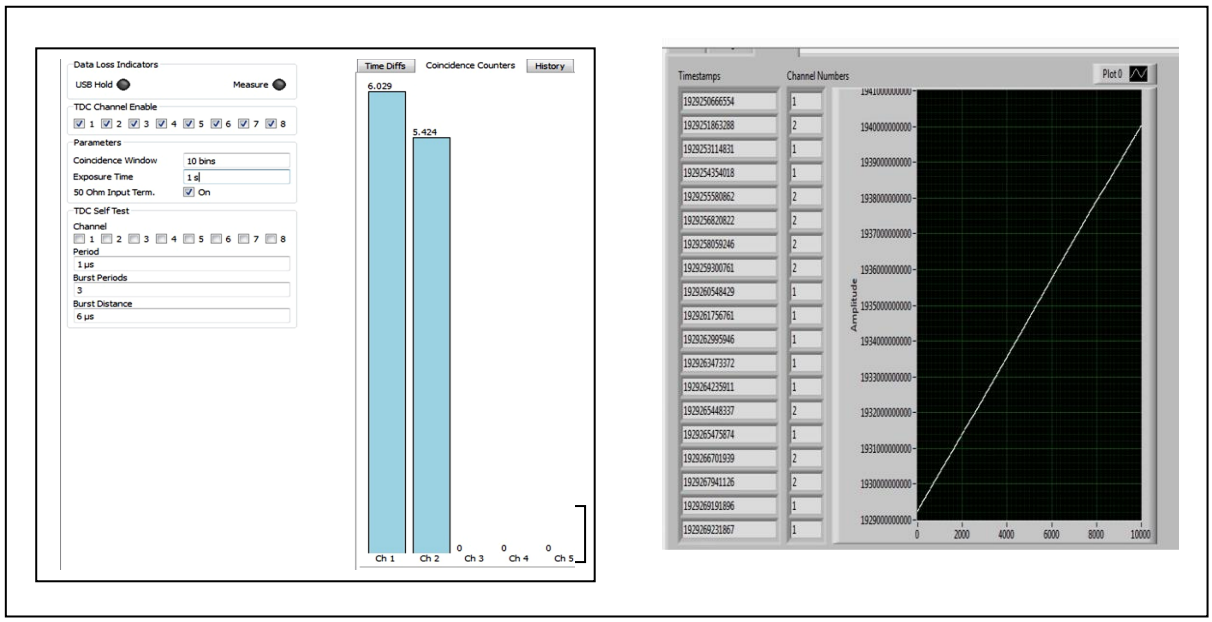

Fig.(13): A 10000 true random sequences recorded at ch1 and ch2 of TDC: (a ,c):counters, (b ,d): time tags

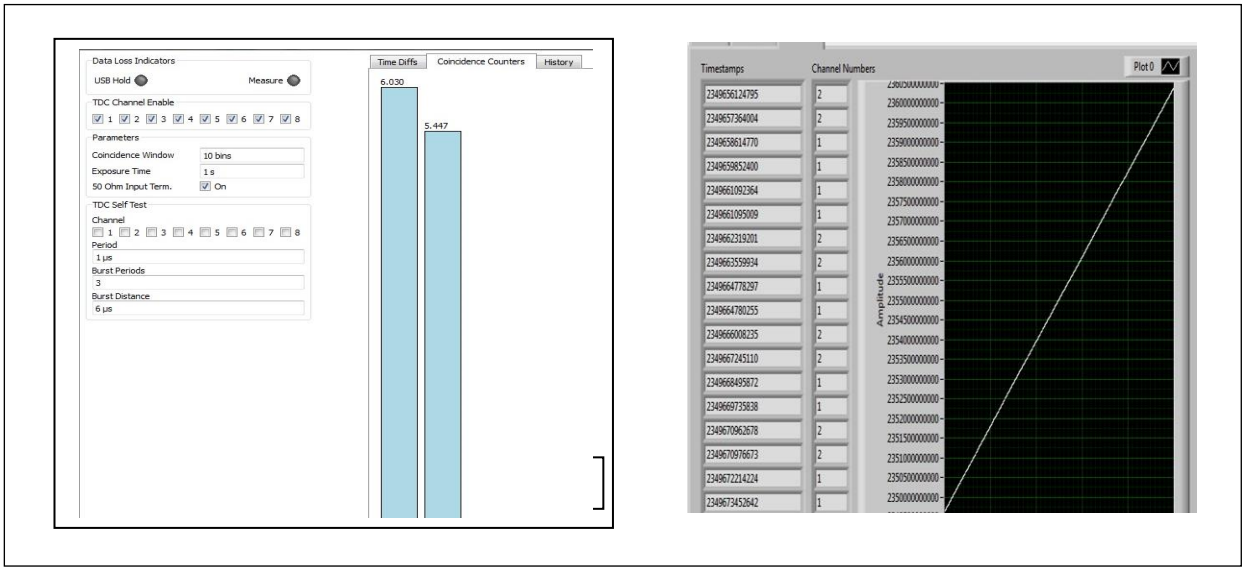

Fig.(13): Continued

Conclusion

A simple random generator of TTL signals to control the operation of laser diodes at transmitters of QKD systems was investigated by using time to digital converter. The true random TTL signals were generated by the Arduino UNO microcontroller controlled the operation of the laser diodes successfully. This true random TTL signal generator can be used to control the operation of four laser diodes for four polarization states of photons transmitted from Alice to Bob in QKD systems based on BB84 protocol, or for both Alice and Bob in MDI- QKD systems and for Bell state measurements in QKD systems based on entangled photons. Using four laser diodes will offer simpler transmitters' design with lower cost compared with transmitters' setups using acousto -optic modulators**,** asymmetrical Mach-Zehnder interferometer and phase modulators.

References

[1] G.B. Xavier, T. Ferreira da Silva, G. Vilela de Faria, G.P. Temporão and J. P. von der Weid, University of Rio de Janeiro

[2] C.H. Bennett and G. Brassard, IEEE Int. Conf. Comput., Syst. Signal Process., 175–179 (1984)

[3] Hong-Wei Li, Zhen-Qiang Yin, Shuang Wang, Yong-Jun Qian, Wei Chen, Guang-Can Guo, and Zheng-Fu Han, nature/Scientific Reports (2015)

[4] R.S. Hasan, S.K. Tawfeeq, N.Q. Mohammed, A.I. Khaleel, Chinese Journal of Physics, 385-391 (2018)

[5] S.K. Tawfeeq, Iraqi J. Laser, Part A, (12) 1-5 (2013)

[6] S.K. Tawfeeq, JOURNAL OF LIGHTWAVE TECHNOLOGY, 27 (24) 5665-5667 (2009)

[7] H.-Q. Ma, Y. Xie, L.-A. Wu, Appl. Opt. 44 (36) (2005)

[8] Simona Buchovecká, Czech Technical University In Prague (2012)

[9] A. Rukhin, J. Soto, J. Nechvatal, et al.,U.S. Department of Commerce (2010)

[10] Zhiyuan Tang, Graduate Department of Physics University of Toronto (2016)

[11] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo, Phys. Rev. Lett**.** 112 (19) (2014)

[12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi, Phys. Rev. Lett. 108 (13) (2012)

[13] Yan-Lin Tang,Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan,Dong-Xu Yang,Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, and Jian-Wei Pan, PRL 113,19 (2014)

توليد اشارات عشوائية لمنظومات توزيع المفتاح الكمي بالأعتماد على متسلسلات عشوائية ثنائية حقيقية

سلوى مروان صالح شيلان خسرو توفيق أحمد أسماعيل خليل

معهد الليزر للدراسات العليا، جامعة بغداد، بغداد، العراق

الخلاصة: تم تنفيذ و التحقق من دوائر مولد اشارات TTL عشوائية لمنظومات توزيع المفتاح الكمي . تم توليد اشارات TTL بدوائر معتمدة على مواد ذات كلفة واطئة و متوفرة في الأسواق المحلية. تم الحصول على اشارات TTL باستخدام متسلسلات ثنائية عشوائية حقيقية بالأعتماد على تسجيل الفرق في زمن وصول الفوتون و المسجل في فترة تطابق بين اثنين من كواشف الفوتون المنفرد. تم اختبار اداء الدائرة الألكترونية باستخدام محول الزمن الى اشارة رقمية و الذي يعطي دقة كبيرة في قياس زمن وصول الفوتون في الأشارات الضوئية التي يتم كشفها في الكواشف البصرية. ممكن استخدام الدوائر المصممة في منظومات عديدة من منظومات توزيع المفتاح الكميلتحقيق االتشغيل العشوائي للمرسلات في هذه المنظومات