Iraqi J. Laser, Part A, Vol.10, pp.1-7 (2011)

IRAQI JOURNAL OF LASER

Generation of Truly Random QPSK Signal Waveforms for Quantum Key Distribution Systems Based on Phase Coding

Shelan K. Tawfeeq and **Ahmed I. Khalil**

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

(Received 3 July 2011; accepted 7 August 2011)

Abstract: In this work a model of a source generating truly random quadrature phase shift keying (QPSK) signal constellation required for quantum key distribution (QKD) system based on BB84 protocol using phase coding is implemented by using the software package OPTISYSTEM9. The randomness of the sequence generated is achieved by building an optical setup based on a weak laser source, beam splitters and single-photon avalanche photodiodes operating in Geiger mode. The random string obtained from the optical setup is used to generate the quadrature phase shift keying signal constellation required for phase coding in quantum key distribution system based on BB84 protocol with a bit rate of 2GHz/s.

Introduction

It is known that a Vernam one-time pad is a cryptosystem with perfect security, where a plain text message is ciphered/ deciphered by a secret key (actually a random bit string) whose bit length is equal to that of the plain message. However, a crucial problem is how to deliver a secret key to two legitimate parties in a secureway.The key has to be discarded after each transmission, since by reusingit Eve can obtain information about the secret message. This is the reason why theVernam cipher is often referred to as the one-time pad. The problem of exchanginga secret key, i.e., the key distribution problem, is the reason why this algorithmhas not been used in cryptographic systems, especially considering the overhead of atrusted courier needed for the exchange of a new key after each transmission.

Theadvent of quantum cryptographygave a solution to the key distributionproblem. The exchange ofsecret keys between Alice and Bob without the need of a trusted courier was achieved by quantum key distribution algorithms. Laws of quantum mechanics guaranteed the security, ensuring that the key can be usedafterwards to encrypt and decrypt messages as a one-time pad for unconditionallysecure cryptography [1].

Fundamental principles of quantum mechanics are used in quantum cryptographyto ensure the security of secret key generation [2]. The first protocol for QC has been proposed in 1984 by Bennett and Brassard, hence the name BB84 under which this protocol is recognized nowadays [3].

A typical system for quantum cryptography using polarization coding is shown in Figure 1. In this protocol ideally, one party (Alice) prepares a sequence of single photons, their polarizations being chosen randomly from four possible non-orthogonal states (e.g. horizontal, vertical and ±45 ◦). She sends the photons to the second party (Bob), who analyses the polarization of each detected photon in a randomly and independentlychosen basis (e.g. either H/V or ±45 ◦). Afterwards both parties compare publicly their basis choices and discard those events where they had used different bases. This process is called sifting [2].

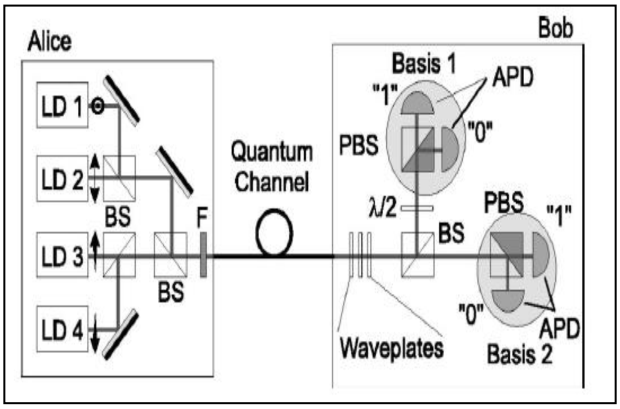


Fig. (1): Typical system for quantum cryptography using polarization coding: **LD**, laser diode; **BS**, beamsplitter; **F,** neutral density filter; **PBS**, polarizing beamsplitter; l/2, half waveplate; **APD**, avalanche photodiode [4].

Although the original proposal of BB84 relies on the polarization state of a photon, phase-encoding BB84 ismainly used these days, because it is inconvenient to use the polarization state as regards fiber transmission [5].

The basic configuration for phase-encoding BB84 systems is shown in Figure 2. Alice transmits a photon through an asymmetric Mach–Zehnder interferometer where the phase difference $\theta_a$between the two paths is randomly chosen from one of four values, namely {0, π}and {π/2, 3π/2}. From theinterferometer, a photon positioned over two time slots is output with a phase difference of θ_a. The photon is sent to Bob. Bob transmits the arriving photon through an interferometer identical to Alice's, in which the phase difference $\theta_b$is randomly chosen from {0, π/2}. The photon isthen detected at the interferometer outputs [5].

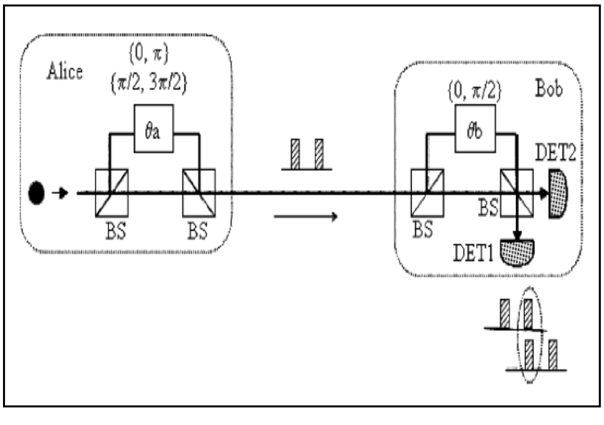


Fig. (2): Basic configuration of phase-encoding BB84 system. DET: Photon detector; BS: beam splitter [5].

Optical QKDsystem is based on the use of single-photon Fock states inwhich any state of the Fock space is with a well-definednumber of particles. Unfortunately, Fock states are ,up to now,difficult to realize experimentally. A more practical choice is using faint laser pulses , i.e. weak coherent states(WCP) or entangled photon pairs, in which both thephoton and the photon-pair number distribution, obey Poissonstatistics.Then the key issue in a QKD system turns to be thedetection of quantum level Qbits, such as the reliable andinexpensive WCP. Today, the Geiger gated-mode avalanchediode, also called photon counter (PC), is widely used. Low and precise temperature control are necessary for the operation of PC, i.e. around -30ºC, and exhibits inherent low quantum efficiency around 0.1and the inevitable residual after-pulse noise due to themacroscopic avalanche at the C band, i.e., 1550nmwidely used in optical communications. Moreover itsoperational frequency is limited to 4-8MHz due to thenecessary quenching process.On the other hand, coherent optical communication is oneof the most promising ways to achieve highest receiversensitivity, excellent spectral efficiency and longesttransmission distance for the next generation of opticalcommunication systems. Already in the late 1980s and early1990s coherent systems attracted a lot of attention as itwas a promising way to improve the receiver sensitivity [6].

In phase coding QKD systems the BB84 protocol requires Alice's choice from two bases, and each base has two symbols. This permits four differentparameter values. In an optical fiber scheme operating with phase modulation, the symbols must have antipodal phasestates in two conjugated bases, and the BB84 requirements can be met by positioning each of these four values as one offour points in a QPSK constellation where the signal waveforms are represented as [7],

$$E_m(t) = E(t)exp\left(j\frac{\pi}{2}(m-1)\right)$$

Where, m=1,2,3,4

Hence Alice generates 4 different phase states to perform this task.Bob has two bases only. The final key obtained depends on the coincidence/anticoincidence between the phase difference between Alice and Bob as listed in Table 1 [8].

Table (1): Implementation of BB84 protocol.Phase and results for the different values of phase corresponding to Alice and Bob's choices [8].

ALICE			BOB			
BASE	**BIT**	Φ_A	**BASE**	Φ_B	$\Phi_A+\Phi_B$	**KEY**
A_1	0	π/4	B_1	-π/4	0	0
			B_2	π/4	π/2	×
	1	5π/4	B_1	-π/4	π	1
			B_2	π/4	- π/2	×
A_2	0	- π/4	B_1	-π/4	- π/2	×
			B_2	π/4	0	0
	1	3π/4	B_1	-π/4	π/2	×
			B_2	π/4	π	1

To practically achieve QKD system giving QPSK constellation points needed by Alice and binary phase shift keying (BPSK) demodulator needed by Bob, twotwo-electrode Mach Zehnder electro-optical modulator (EOM) can be utilized. This type of modulator is composed bytwo directional couplers; the first divides the incident beam into two parts and the second combines the parts aftercontrolled phase-shifted propagation. It is possible to change the path in each arms by applying a voltage acrossthe wave-guide in each arm, and to control the optical phase shift in wave-guides as shown in Figure 3. Bob adds to the field a new phase variation permitting to extract the base choices and symbol information as established in the BB84 protocol [9].

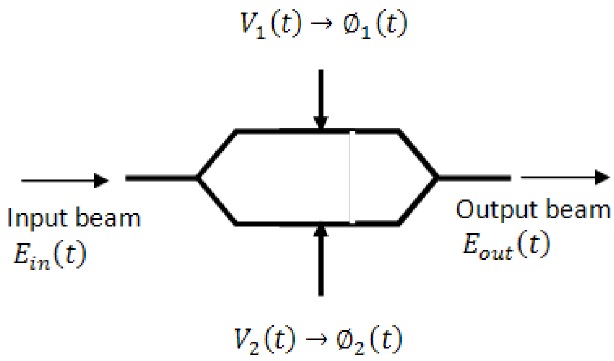


Fig.(3): Integrated Mach-Zehnder modulator with two Electrodes [8].

Figure 4 shows the setup used to generate the truly random binary sequence. It consists of a laser diode (LD) operating with a wavelength of

The variation in both amplitude and phase, depending on the signals introduced to eacharm following the equation [9]:

$$E_{out}(t) = E_{in}(t).\cos\left(\frac{\emptyset_1-\emptyset_2}{2}\right) exp\left(j\frac{\emptyset_1+\emptyset_2}{2}\right) \quad (1)$$

where,

$\emptyset_1 and\ \emptyset_1$are the phase shifts induced by the modulation tension applied in electrode 1 and 2 respectively.

At Alice's side,
$\left(\frac{\emptyset_1+\emptyset_1}{2}\right)$ =Φ_A

In order to generate the QPSK signals at Alice side and keep the intensity constant, i.e.,
$\emptyset_1 - \emptyset_2 = \mp\frac{\pi}{2}$

At Bob's side just one electrode of Mach-Zehnder is used to apply an electrical signal related to Φ_B.

Experiment and Results

The experiment was directed into two directions. First, building an optical setup to generate truly random sequence of binary bits at Alice's side. Second, generating the attenuated QPSK signal constellation also at Alic's side that can be used in any QKD system based on BB84 protocol.

650 nm with an output power of 1 mW, repetition rate of 11 kHz, pulse width of 200 ns. The average number of photons per pulse (μ) for

this laser diode was adjusted to be equal to 0.24. This was achieved by attenuating the output optical power of the LD. For this value of μ , the attenuated average optical power of the LD was equal to 20.16 nW.Attenuating the output power for this LD is necessary to ensure that the output power obeys Poisson statistics in order to achieve that the single- photon APDs operating with Geiger mode do not saturate. The LD output power which consists of number of photons will be divided equally by the first beam splitter (BS1). For each photon there is a probability of 50% to be reflected by the BS and a 50% probability to be transmitted through the BS. That means the optical beam will be equally divided into two parts by BS1. The same process will occur at BS2 and BS3. Four single-photon avalanche photodiodes (APD) working in the Geiger mode were used for detection of the photons in four paths. The detection time for the photons was controlled by building some electronics circuits that provide a 1 μs window for detecting the first APD that detects a photon, so that the other readings will be neglected.By using four single-photon avalanche photodiodes, four states can be obtained, i.e., APD click represents a state, APD1,APD2,APD3 and APD4 corresponds to states 1, 2, 3 and 4 respectively. These detection results are stored in a personal computer and then states are converted to binary numbers, 00, 10, 01 and 11 by a MTALAB program to represent the QPSK constellation states. These binary numbers are then converted to a string that will be fed to the sequence generator of the OPTISYSTEM simulation package.

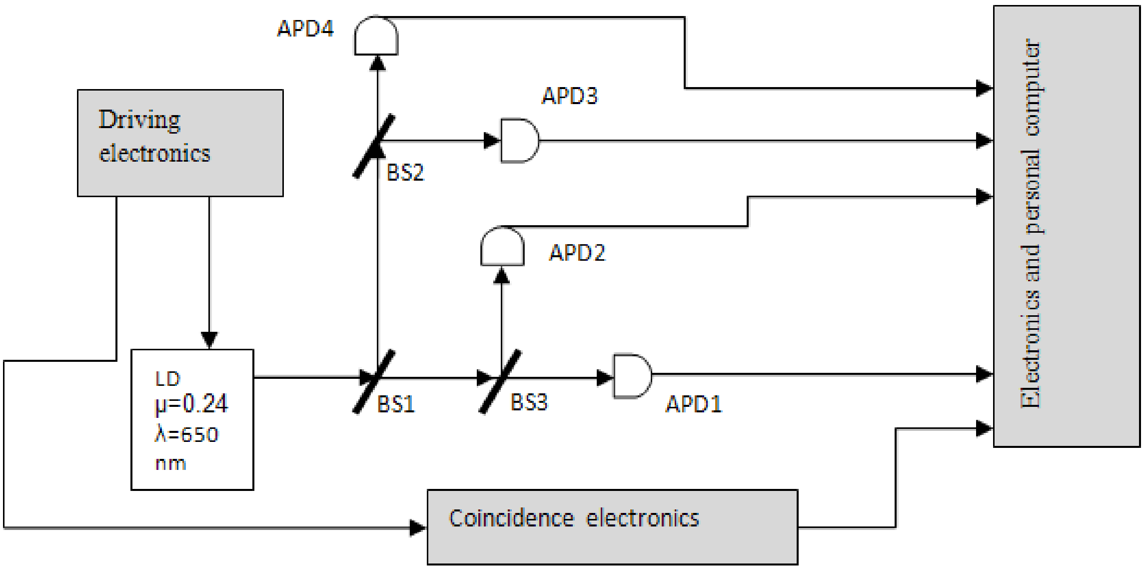


Fig. (4): The optical setup for generating the random input sequence. APD: single photon avalanche photodiode. BS: beam splitter. LD: laser diode.

Figure 5 represents the block diagram that was implemented by using the OPTISYSTEM simulation package. The random bit sequence generator takes its data from the file that includes the random binary stream that was obtained from the optical setup shown in Figure4. This binary stream is used to operate the PSK signal generator that takes two bits from the random binary sequence generator each time. Then to obtain the QPSK signal, the PSK signal generator will send each odd-numbered bit to one of the M-ary signal generators and the even-numbered bits to the other M-ary signal generator. By using M-ary signal generators a multi-level signal is obtained that is used as external signals for the Mach-zehnder modulators for modulating the laser signal operating with a wavelength of 1550 nm and output power of 0dBm. Two Mach-Zhenders are used to obtain the QPSK signal constellation.The QPSK waveform obtained is attenuated to get optical power in the range of (2-8) nW , 41 dB attenuation, to have weak coherent pulses necessary for quantum cryptography.

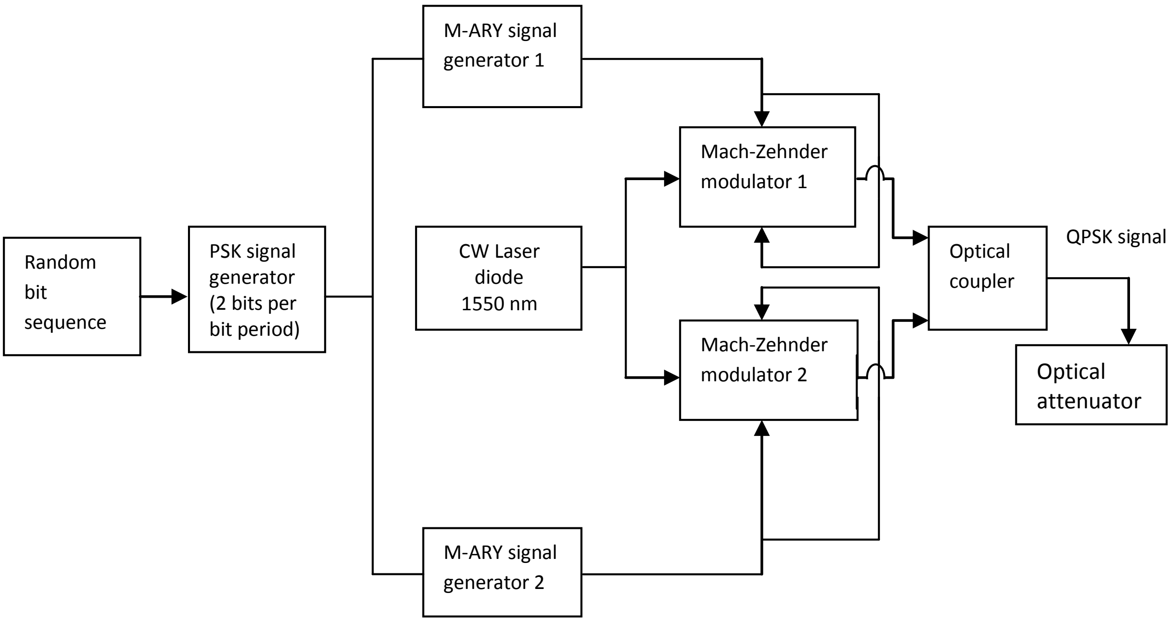


Fig. (5): The setup model to generate QPSK signal waveforms at Alice's side

Figure 6 shows the waveform of random bit sequence generator operated by the random sequence obtained from the optical setup shown in Figure 4.The bit rate is 2GHz/s. Figure 7 shows the M-ary pulse generators waveforms.Figure (8) shows the QPSK signal waveform at the output of the coupler at Alice's side and the attenuated QPSK signal waveform. It is clear from the Figure that there are four levels of optical power each level represents the voltage required to obtain a specific value of a phase required by Alice, as listed in Table 1, to apply BB84 protocol. These levels of voltages can be changed by changing the parameters of the Mach-Zehnder modulator, i.e., changing the modulation voltage values, as shown in Figures 8-a and 8-b.

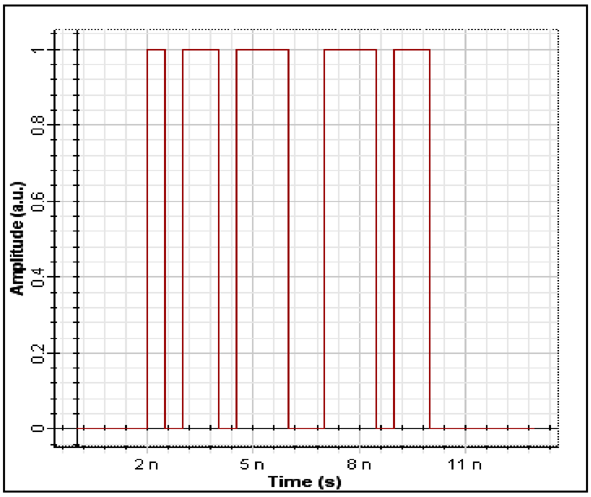


Fig.(6): Random bit sequence

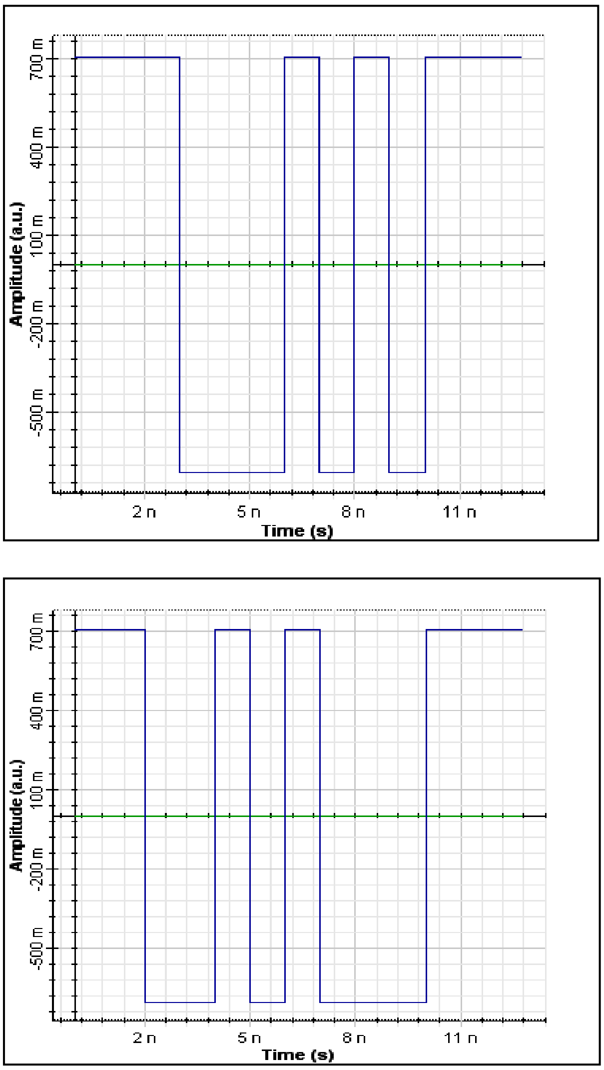
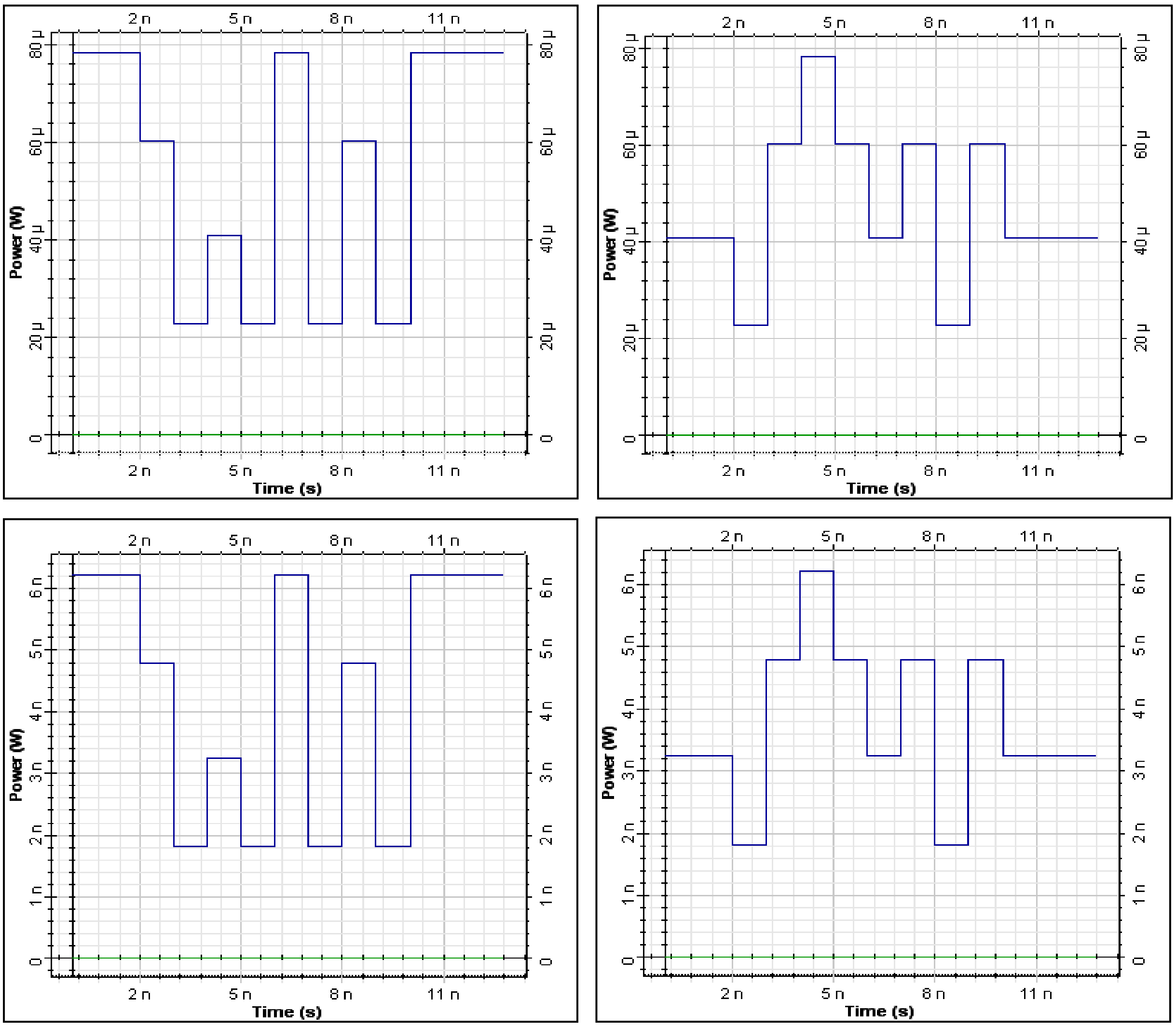


Fig. (7): M-ary pulse generators waveforms



(a) (b)

Fig. (8): QPSK signal waveform, a) Mach-Zehnder 1: modulation voltage 1= -1 V, modulation voltage 2=1 V, Mach-Zehnder 2: modulation voltage 1= -0.5 V, modulation voltage 2=0.5 V. b) Mach-Zehnder 1: modulation voltage 1= 1 V, modulation voltage 2= -1 V, Mach-Zehnder 2: modulation voltage 1= 0.5 V, modulation voltage 2=-0.5 V.

Conclusions

A truly random QPSK signal waveforms for quantum key distribution systems based on phase coding is implemented. This model can be practically implemented and used in optical fiber communication systemsworking with 1550 nm laser sources. The key generated is totally random where it is generated depending on the laws of quantum mechanics using the beam splitters with weak coherent optical signals.

References:

[1] E. Diamanti, "Security and implementation of differential phase shift quantum key distribution systems, "Ph.D. thesis, Stanford University, June 2006.

[2] 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, pp. 840 – 845, 2006.

[3] L. Huang, "Long-Distance Quantum Key Distribution over TelecomFiber, " M.Sc. thesis, University of Toronto, 2006.

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, " Quantum cryptography," Reviews of Modern Physics , ***74***, , pp.145 – 195, Jan. 2002.
[5] K. Inoue, "Quantum Key Distribution Technologies," IEEE J. OF Selected Topics in Quantum Electronics, ***12***, No. 4,pp 888- 896, JULY/AUG. 2006.
[6] Q. Xu, M.Sabban, P.Gallion and F. Mendieta, " Quantum Key Distribution Systemusing Dual-threshold Homodyne Detection,"Research, Innovation and Vision for the Future, 2008. RIVF 2008. IEEE International Conference, 13-17 July 2008.
[7] M.B. Silva, Q. Xua, S. Agnolinia, P. Galliona, F.J. Mendieta, " Homodyne detection for quantum key distribution: an alternative to photon counting in BB84 protocol," Proceedings of Spie, ***6343***, June 5-8 2006
[8] S. Agnolini and P. Gallion, " Implementation of BBS4 protocol by QPSK modulation using dual-electrode Mach-Zehnder modulator," IEEE International Conference on Industrial Technology (KIT), 2004.
[9] Q. Xu, " Optical homodyne detection and applications in quantum cryptography," Ph.D. thesis, Telecom Paris Tech, 2009.

توليد موجات اشارة تغيير ازاحة الطور الرباعي العشوائية الحقيقية لمنظومات توزيع المفتاح الكمي بالأعتماد على تشفير الطور

شيلان خسرو توفيق **احمد اسماعيل خليل**

معهد الليزر للدراسات العليا، جامعة بغداد ، بغداد ، العراق

الخلاصة

في هذا العمل تم بناء نموذج لمصدر يولد توزيع اشارة تغيير ازاحة الطور الرباعي العشوائية المطلوبة في منظومات توزيع المفتاح الكمي المتعلقة ببروتوكول BB84 المستخدم لتجفير الطور بواسطة استخدام برامجيات OPTISYSTEM 9 . العشوائية للسلسلة المتولدة تتحقق ببناء منظومة بصرية معتمدة على مصدر ليزري خافت، مقسمات ضوء و كواشف فوتونات منفردة ذات الأنهيار المضاعف تشتغل بالنمط كايكر. السلسلة العشوائية المتولدة من المنظومة البصرية تستخدم لتوليد اشارة تغيير ازاحة الطور الرباعي المطلوبة لتشفير الطورفي في منظومة توزيع المفتاح الكمي المتعلق ببروتوكول BB84 بمعدل وحدة ٢ كيكا وحدة في الثانية.