International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-6)

Research Article | **June 2014**

Dual Quantum Random Number Generator using a FPGA for QKD-CV systems: Preliminary results

Dr. Josué Aarón López Leyva
Head of Cybernetic and Mechatronics Engineering
CETYS University &university

Abstract—

This paper presents the preliminary results of a dual quantum random number generator using a FPGA DE0 Nano and optical set-up experiment with variable transmission rate from 10 to 50 Mbps using coherent detection to detect the quadrature components in a simultaneously way of an optical vacuum state using a 90 degree optical hybrid. The main application for this type of system is the quantum cryptographic systems of second generation and all activities where two random sequences requiring speeds of about 50 Mbps are necessary. Finally, the performance of the overall systems is determined measuring the bias probability (0.0002±0.000001) of the finals random binary sequences.

Keywords— Quantum states, coherent detection, quadrature components, FPGA, random numbers generator

I. INTRODUCTION

The truly random numbers generators systems are very useful in various applications such as games lottery, casinos, etc. [1, 2]. In the particular case, these systems are necessary for security application which is required to encrypt the information due to the high importance of the data sent, such as bank account passwords [3]. Currently there are different schemes of cryptography systems, where the essential subsystem is a random number generator to produce a random key and so minimize the probability that the information is stolen. However, due to the physical and technical limitations of the most encryption systems using pseudorandom number generators via a computer or dedicated digital card; these systems do not actually show truly random binary sequences due to the use of complex mathematical functions or some source of pseudo-random noise such as a thermal noise, which under specific conditions is not random [4]. In order to increase the security level and transmission rate of traditional cryptography systems have emerged latter other cryptography systems considering the physicals laws which are classified into first generation systems or DV-QKD (Discrete Variables Quantum Key Distribution) and second generation or CV-QKD (Continuous Variables Quantum Key Distribution) having more acceptance CV-QKD due to the common technological devices used. In the specific case of the quantum cryptography system with continuous variables commonly is modulated the amplitude and phase of an optical quantum state in four different levels, so, two truly random binary sequences are necessary (a generator drives the amplitude and other the phase) or some electronic adaptation using only a random generator, however involves a trade-off to reduce by half the total transmission rate of the generator, so that is required a faster generators, increasing the cost of the final product or service. A variant of the CV-QKD systems are those that only modulate the phase and not the amplitude of a Weak Coherent State (WCS) using a conventional QPSK (Quadrature Phase Shift Keying) modulation scheme where each quadrature components represents a specifically base in the cryptography context [5].

This paper shows the set-up experiment and preliminary results of a dual quantum random number generator system considering the information of both quadratures components of an optical vacuum state using coherent detection and a DSP block using a FPGA DE0 Nano.

II. SET-UP EXPERIMENT AND PRELIMINARY RESULTS

The experimental set-up is shown in Fig. 1. In roughly speaking, there are exists two parties in quantum cryptography context; the transmitter system called Alice and receiver system called Bob. Alice is composed of two subsystems; the dual true random generator (DUAL TRNG) and the optical phase modulation scheme for WCS, after, the quantum key have to send through private channel using a dedicated fiber optic link. In a same time, the encrypted data information is sending using a classical network (public channel). In this paper the technical details of Bob are not shown but generally, Bob is a system with simultaneous quadrature detection using coherent detection scheme [6]. A laser at 1550 nm was used to generate two signals; one signal is to generate the

random binary sequence and the other for transmission over the private channel. With respect to Dual QRNG, a 90 degree optical hybrid was implemented to detect quadrature components in a simultaneously way of the optical quantum vacuum state using coherent detection. The outputs signal of the BHDs give random information about the quadrature components of the vacuum state, this information is processed using ADC built-in in a FPGA DE0 Nano of 12 bits in order to generate a two truly random digital sequence. Due to the clock of the FPGA is 50 Mbps, the transmission rate of the two truly random digital has a dynamic range from 10 to 50 Mbps. After, the random sequences were used as the driver signals for the phase modulator. Because the BHDs bandwidth is 5 MHz, was necessary the design of a buffer in the FPGA using VHDL (Very High Speed Integrated Circuit Hardware Description Language) a prior to generating the final random sequence with the adequate length.

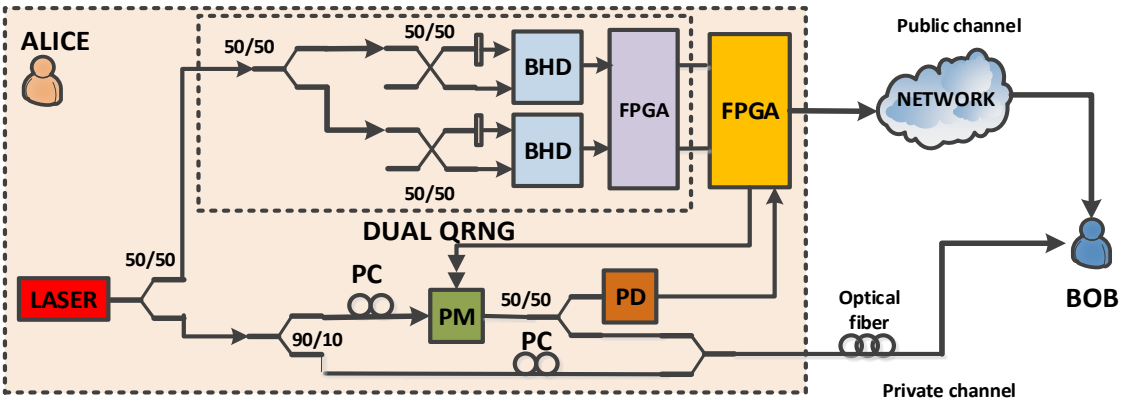

Fig. 1. Set-up experiment. PC: polarization controller, PM: phase modulator, PD: photodetector, BHD: balanced homodyne detector, DSP: digital signal processing block, FPGA: field-programmable gate array.

order to determine the overall performance of dual QRNG, several parameters can be measured, in our case was used the bias probability at each final sequence generated using Matlab post-processing. The bias probability can be determined by considering each probability of symbols and final bits of the overall scheme, in addition the QPSK system can be separated for practical reasons into two BPSK systems , such that:

$$bp\text{–}inphase = p(00) - p(01)$$
$$bp\text{–}quadrature = p(10) - p(11)$$

,where $p(00)$, $p(01)$, $p(10)$ and $p(11)$ represents the probability in each symbol, $bp\text{–}inphase$ and $bp\text{–}quadrature$ represent the bias probability in the quadrature components. In particular, Figure 2 shows the experimental results of 100 measurements (one measurement per second) considering a transmission rate at 10 Mbps of the bias probability in the in-phase component.

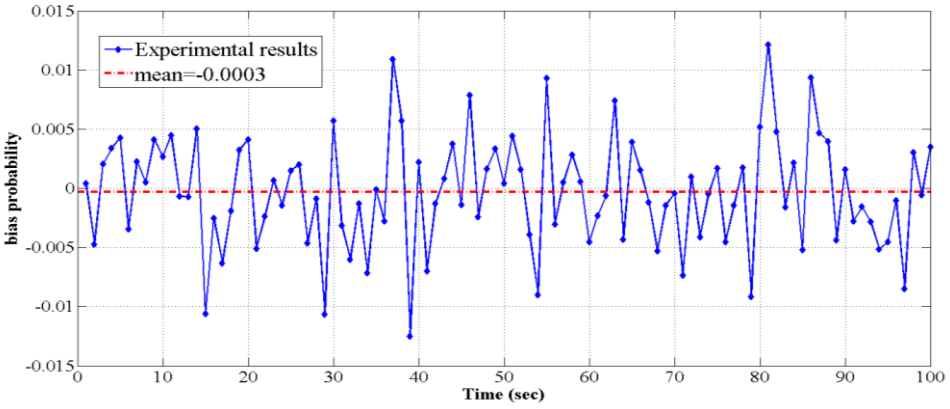

Fig. 2. Experimental results of the bias probability of the in-phase component.

The results shown in Fig. 2 only represent the bias probability of a random binary sequence that modulates the in-phase component of the optical signal transmitted for the private channel. Also is possible to measure the bias probability for the other sequence that modulate the quadrature component, however, was preferred measure the bias probability of the overall QPSK constellation. The table 1 shows the value of the bias probability considering the complete constellation using 10,000 samples per symbol normalized to the shot noise units (i.e. the variance of the vacuum state such reference of modulation level) for different transmission rates. Finally, the bias probability value considering the complete constellation was 0.0002±0.000001for 100 measurements.

TABLE I
BIAS PROBABILITY IN QUADRUTURE COMPONENTS FOR DIFFERENTS TRANSMISSION RATES

Bit rates (Mbps)	**bp-inphase**	**bp-quadrature**
10	0.00029±0.000001	0.0003±0.000001
20	-0.0003±0.000001	0.00029±0.000001
30	0.00031±0.000002	0.00031±0.000001
40	0.00029±0.000001	-0.0003±0.000001
50	0.0003±0.000001	0.00029±0.000002

III. CONCLUSIONS

In this paper a dual generator truly random binary generator using the vacuum noise of a quantum optical state was presented. A 90 degree optical hybrid was used for measured in a simultaneously way the quadrature components of the vacuum state that are truly random. Also a FPGA DE0 Nano was used for obtain the final binary sequences with variable transmission rates from 10 to 50 Mbps. The system shows an adequate performance with respect to the bias probability, 0.0002±0.000001 average, however, others measurements are necessary to ensure the randomness

ACKNOWLEDGMENT

A cordial gratitude and acknowledgment to CETYS University for the administrative and technical support for this research project.

REFERENCES

[1] Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed.: John Wiley & Sons, 2001.

[2] Blaner, B., Abali, B. Bass, B.M., Chari, S., Kalla, R., Kunkel, S., Lauricella, K., Leavens, R., Reilly, J.J., Sandon, P.A.:
"IBM POWER7+ processor on-chip accelerators for cryptography and active memory expansion", *IBM Journal of Research and Development*, 2013, 57, 6, pp.1-16, 10.1147/JRD.2013.2280090.

[3] M. Stipčevića and B. Medved Rogina: "Quantum random number generator based on photonic emission in semiconductor", *Review of scientific instrument*, 2007, 78, pp. 1-7, doi: 10.1063/1.2720728.

[4] Stipcevic, M.: "Quantum random number generators and their use in cryptography", *MIPRO, 2011 Proceedings of the 34th International Convention*, May 2011, pp.1474-1479, 12137617.

[5] Oesterling, L., Hayford, D.,Friend, G., "Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information", *IEEE Conference on Technologies for Homeland Security (HST),* 13-15 Nov. 2012, pp. 156 – 161.

[6] J.A López, A. Arvizu, E. García, F.J. Mendieta, E. Álvarez, P. Gallion. "Detection of phase-diffused Weak-Coherent-States using an Optical Costas Loop.", *Optical Engineering*, Vol. 51, No. 10, Octubre 2012. doi: 10.1117/1.OE.51.10.105002

