ISSN (EN LINEA): 1850 - 1158

# FUENTE CUÁNTICA ÓPTICA DE NÚMEROS ALEATORIOS

# OPTICAL QUANTUM RANDOM NUMBER SOURCE

**H.E. Benítez[1], L.A. Perez[1], Ch.T. Schmiegelow[1], M.G. Kolvalsky[2], M.A. Larotonda[2*] y A.A. Hnilo[2]**

[1]Departamento de Física J.J.Giambiagi, (FCEyN) - Universidad de Buenos Aires.
Pabellón I, Ciudad Universitaria - (1428) – Cdad. Bs. As. - Argentina
[2]Centro de Investigaciones en Láseres y Aplicaciones (CONICET –CITEFA).
J.B. de La Salle 4397 - (1603) – Villa Martelli-Bs. As. - Argentina
*e-mail: mlaroton@gmail.com*

En este trabajo presentamos un generador de números al azar no determiníistico basado en la naturaleza probabilística de la evolución de un sistema cuántico: un haz de luz de muy baja intensidad se hace incidir sobre un separador de haz formado por los extremos de dos fibras ópticas de longitudes diferentes. A partir de ese momento los fotones pasan a estar en una superposición de los estados "fotón en fibra larga" y "fotón en fibra corta". Al detectar estos fotones con un fotodiodo de avalancha e identificarlos por su tiempo de llegada se produce un colapso de la función de onda en uno de estos dos estados, que se interpretan como bits en estados "0" y "1" respectivamente.

Palabras Clave: óptica cuántica, generador físico de números aleatorios, información cuántica.

We present a nondeterministic random number generator based on the probabilistic nature of the evolution of a quantum system: A light beam with very low intensity impinges upon a beam splitter formed by the ends of two optical fibers with different lengths. As a consequence, photons are left in a superposition of states "photon in long fiber" and "photon in short fiber". Detecting these photons with an Avalanche Photodiode and identifying them by its arrival times collapses the wavefunction into one of these two states, which in turn are interpreted as bits in states "0" and "1" respectively.

Key Words:quantum optics, physical quantum random number generator, quantum information.

## I. INTRODUCCIÓN

La necesidad de disponer de números aleatorios surge en varias aplicaciones, como por ejemplo el muestreo estadístico [1], las simulaciones por computadora, las apuestas y, sobre todo, la criptografía.

Los *generadores pseudoaleatorios* son algoritmos determinísticos que intentan generar objetos aleatorios grandes a partir de una *semilla* aleatoria más corta. Si bien resultan útiles y confiables para la simulación [2] y el muestreo, no existe garantía de su confiabilidad para el manejo seguro de la información [3].

Por esta razón, la generación y transmisión de claves criptográficas requiere la utilización de una fuente *objetiva* de aleatoriedad.

Las fuentes físicas de números aleatorios utilizan la aleatoriedad de un observable físico, por ejemplo el ruido de una señal o de un dispositivo electrónico. Algunos generadores físicos utilizan fenómenos cuya complejidad implica un comportamiento caótico aunque en sentido estricto determinista y no aleatorio (ejemplo: movimiento de las partículas de polen en la superficie de un fluido).

La teoría cuántica, por su parte, nos permite pensar en fuentes objetivamente aleatorias. Tomemos el experimento de difracción de doble rendija (Fig. 1), que cuenta con una fuente de partículas (*e.g.* fotones, neutrones o electrones), un arreglo de dos rendijas y una pantalla de observación en un plano a cierta distancia.

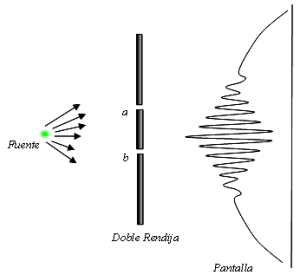


*Figura 1: Interferencia de doble rendija.*

Cuando se lleva cabo el experimento, se observan en la pantalla franjas de interferencia, explicadas por el comportamiento ondulatorio de las partículas emitidas por la fuente. Estas franjas de interferencia se observan aún cuando la fuente se atenúa de tal forma que las partículas llegan a las rendijas de a una a la vez, es decir que surgen por la interferencia de cada partícula consigo misma [4].

Desde el punto de vista de la mecánica cuántica no hay forma de saber, al observar el patrón de interferencia,

* Autor a quién debe dirigirse la correspondencia.

por cuál de las dos rendijas pasó la partícula. Si se fuera a realizar un experimento para determinar el camino tomado por la partícula, se debe interactuar con ésta de alguna manera, llevando a la decoherencia, i.e. a la pérdida del patrón de interferencia. Sólo cuando no hay forma de saber, aún en principio, a través de qué rendija pasó la partícula se observa el patrón de interferencia.

Cuánticamente entonces, el estado de la partícula es la superposición coherente $|\Psi\rangle = 1/\sqrt{2}\left(|\Psi_a\rangle + |\Psi_b\rangle\right)$, donde $|\Psi_a\rangle$ y $|\Psi_b\rangle$ representan los estados cuando sólo está abierta la rendija a o b respectivamente. De manera general, el estado para un sistema cuántico en superposición de estados puros $|\Psi_a\rangle$ y $|\Psi_b\rangle$ se escribe:

$$|\Psi\rangle = \alpha|\Psi_a\rangle + \beta|\Psi_b\rangle \qquad (1)$$

con $|\alpha|^2 + |\beta|^2 = 1$. Si se prepara entonces un sistema cuántico en el estado general de superposición (1), se obtiene un fuente física de aleatoriedad: al medir se obtendrá el estado $|\Psi_a\rangle$ con probabilidad $|\alpha|^2$ y el estado $|\Psi_b\rangle$ con probabilidad $|\beta|^2$. Llamando $|0\rangle$ y $|1\rangle$ a $|\Psi_a\rangle$ y $|\Psi_b\rangle$ respectivamente tenemos una fuente física de bits al azar con las correspondientes probabilidades $|\alpha|^2$ y $|\beta|^2$.

medición se realiza acoplando un detector de fotones a la salida de las fibras.

A partir de estas mediciones, utilizando dos fibras *a* y *b* de distintos largos $l_a$ y $l_b$ tenemos dos caminos ópticos de diferente longitud por lo que registrando los tiempos de arribo podemos asignar un estado $|\Psi_a\rangle$ y $|\Psi_b\rangle$ a los fotones detectados.

El dispositivo experimental se observa en la Figura 2. Un objetivo de microscopio enfoca la luz de la fuente (LED) sobre una fibra óptica monomodo. El haz de luz de salida incide sobre un par de fibras ópticas multimodo muy cercanas entre sí (Fig. 2), una de las cuales es de mayor longitud que la otra [$l_a$=(0.31±0.01)m y $l_b$≈150m respectivamente], constituyendo así un camino largo y uno corto. A la salida de las fibras multimodo se emplea nuevamente un objetivo para colimar la luz de las dos fibras sobre el detector.

El detector utilizado es un módulo contador de fotones únicos SPCM-AQR-13-FC de PerkinElmer, que consiste de un fotodiodo de avalancha (APD) de silicio, un amplificador, un discriminador y un formador de pulsos TTL.

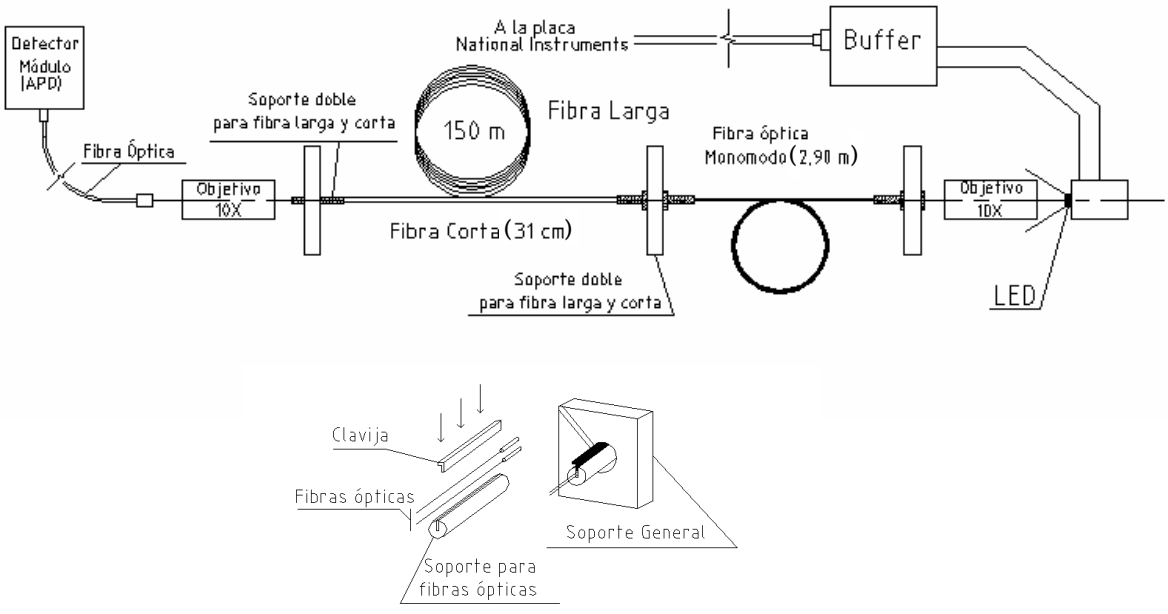


*Figura 2: Dispositivo Experimental. Detalle del Soporte para fibras ópticas.*

## II. MÉTODOS

### A. Dispositivo Experimental

Nuestro objetivo es básicamente lograr una implementación práctica del experimento de doble rendija. Para ello, tomando como referencia el trabajo de Stefanov et al. [5], hacemos incidir un haz de luz sobre un par de fibras ópticas pegadas que actuarían como las rendijas del experimento mencionado. La

Las cuentas de oscuridad (ruido) de este detector siguen un proceso estadístico con distribución de Poisson con un promedio de 236 cuentas por segundo. La eficiencia cuántica típica del detector a 650nm es de 65% sobre el área circular activa de 180μm de diámetro.

El pulso de salida del APD tiene un ancho temporal de 35ns y un tiempo muerto de 60ns, de manera que el menor desfasaje posible entre dos pulsos consecutivos generados por el APD es de 95ns.
Los pulsos TTL del detector son adquiridos por una tarjeta de conteo National Instruments 6602 y procesados con un programa desarrollado en el entorno LabView. El encendido y el apagado del LED está controlado por la misma placa National Instruments.
Se confeccionó un *driver* electrónico con lógica TTL para controlar el LED, que interviene como acoplador para no exigir a la placa en corriente. El mismo consiste básicamente en una compuerta lógica del tipo YES (Fig. 3) que toma una señal de 0-5V (1 y 0 lógico) y la repite a la salida.
Este dispositivo entrega una onda cuadrada con suficiente corriente para alimentar al LED (Fig. 3).
La compuerta tiene una frecuencia de repetición de 10MHz (100ns) y una velocidad de respuesta de 14ns.
La importancia de la forma y estabilidad de la señal de corriente que alimenta el LED es primordial para no producir solapamiento en la estructura de los histogramas de tiempos de llegada obtenidos. En caso de que el *rise time* y el *fall time* del pulso sean largos, los intervalos modales del histograma tienden a solaparse y no pueden distinguirse por tiempo de arribo.

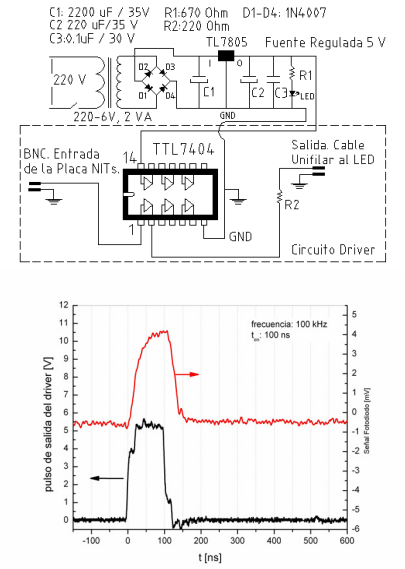


*Figura. 3: Circuito electrónico para controlar el LED. Arriba: diagrama del circuito. Abajo: pulso de salida de período 100ns. Traza superior: pulso de luz emitido por el LED. Traza inferior: pulso eléctrico de alimentación del LED.*

**B. Obtención de Datos.**

Para la generación de los eventos es necesario primeramente que la alineación del dispositivo sea tal que minimice las perdidas de luz desde el LED hasta la fibra de entrada del detector. Por la configuración de nuestro dispositivo existen tres sectores a alinear. En primer lugar se pretende perder la menor cantidad de luz posible de la salida del LED a la entrada de la fibra monomodo. Para tal fin se ubica un objetivo 10X sobre el eje longitudinal a 5±1 mm desde la salida del LED y a 16±1 mm de la fibra monomodo (aproximadamente la distancia focal del objetivo). En segundo lugar, el de haz de salida de la fibra óptica monomodo debe acoplarse a las entradas de las fibras multimodo (figura 4).

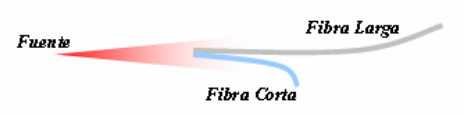


*Figura 4: La entrada de las fibras multimodo se ubican en una región transversal de intensidad homogénea.*

Al ubicar las fibras prácticamente pegadas (y como se trata del mismo tipo de fibra) tenemos que la probabilidad de que un fotón emitido caiga sobre cada una de ellas es muy similar ($|\alpha|\approx|\beta|$ en (1)). La fibra monomodo le quita además cualquier posible dinámica espaciotemporal o deriva al modo del haz ($\alpha$ y $\beta$ se independizan de posibles variaciones de intensidad espacio temporales de la fuente, que podrían introducir eventuales correlaciones entre los bits). Por último, a la salida de las fibras multimodo ubicamos un objetivo igual al anterior para enfocar el haz de salida sobre la entrada de la fibra del módulo contador de fotones.
Se procede a una calibración fina del dispositivo; para ello se realiza una alineación de cada etapa del sistema en forma sucesiva, buscando maximizar la intensidad de luz que llega al contador de fotones, sin sobrepasar el límite soportado por el APD, aproximadamente $10^7$ cuentas por segundo.
Con el dispositivo así configurado procedemos a levantar los primeros histogramas correspondientes a los tiempos de llegada de los fotones al detector. Pulsamos el LED a una frecuencia de 10kHz (T=100μs) con pulsos de 80ns de duración, y levantamos un histograma de los tiempos de llegada de los fotones al detector con un osciloscopio Tektronix TDS 5032B, de ancho de banda de 350MHz. Este osciloscopio nos permite generar un histograma de tiempos de llegada (*hits in the box*) relativos al pulso de disparo, que es el pulso de encendido del LED.
Una incorrecta alineación del sistema puede generar una proporción despareja, o sesgo, entre unos y ceros. Si bien tenemos un algoritmo para balancear los bits obtenidos, cuanto más sesgado sea el punto de partida menos información útil se podrá extraer de la ristra de bits original. Por lo tanto pretendemos una alineación inicial del dispositivo que presente histogramas más simétricos y por ello se procede a un ajuste fino de los posicionadores. En la Figura 5 se presenta un histograma obtenido tras el ajuste mencionado. Una vez que se ha logrado un grado aceptable de simetría se procede a la obtención de las listas de tiempos de llegada.
Debe tenerse en cuenta que se pretende asignar probabilidades a la elección cuántica de camino de cada fotón **individual** que arriba en el estado superpuesto (1). Para ello se atenúa (desenfocando ligeramente en el eje longitudinal) la llegada de luz a las fibras multimodo

de manera que por cada diez pulsos que lleguen al LED se detecte en promedio un solo evento. De esta manera la probabilidad de un evento múltiple es $\approx 0.1^2 = 0.01$. Registrando al mismo tiempo un archivo con los tiempos de arribo y otro con los tiempos en que se emiten los pulsos, simplemente se compara el tamaño (espacio en disco) de los archivos (≈ 1/10).

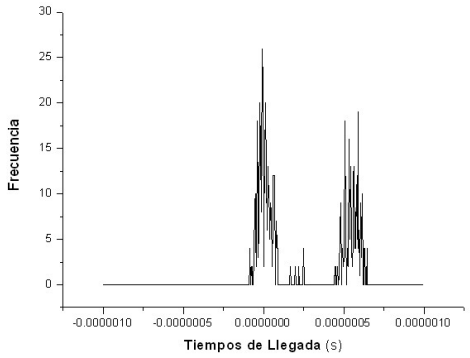


*Figura 5: Histograma simétrico obtenido tras la alineación fina. Ambos eventos tienen una frecuencia de ocurrencia similar.*

La velocidad de generación de datos máxima obtenida fue en general cercana a 16KHz (para T=6.4μs), que es aproximadamente lo esperado (15,625KHz) para el período fijado, teniendo en cuenta la tasa de 0.1 fotones detectados por pulso.

### C. Automatización del dispositivo.

El método recién descrito para la extracción de bits requiere una serie de operaciones algebraicas sobre las listas de tiempos de llegada, lo que nos impide obtener bits en tiempo real. Para sortear este obstáculo incluimos un par de detectores de coincidencias a la salida del APD, como se muestra en la Figura 6. Las coincidencias se detectan en sendas ventanas temporales de manera que cada detector corresponde a uno de los eventos, "fotón fibra corta" y "fotón fibra larga". Así obtenemos directamente listas de 1 y 0.

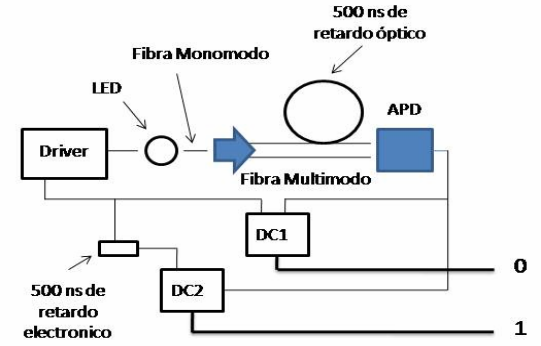


*Figura 6: Esquema del dispositivo automatizado.*

Esta configuración permitió llevar la velocidad de adquisición hasta 25 KHz ya que se elimina la influencia del *afterpulsing* del APD [6].

## III. RESULTADOS Y ANÁLISIS.

### A. Extracción y Procesamiento.

La lista de tiempos de llegada consiste en números enteros que representan ciclos de reloj de la placa adquisidora. Como sabemos que los pulsos enviados al LED se repiten en este caso con un período de 12.8μs (1024 ciclos de reloj a 80MHz), podemos obtener los tiempos de llegada relativos simplemente tomando el resto módulo 1024 en la lista almacenada por el LabView.

Con estos tiempos relativos se construye un histograma de tiempos de llegada (Fig. 7). En dicho histograma observamos la existencia de dos intervalos modales bien definidos. Cada intervalo modal corresponde a uno de los dos eventos posibles, que son fotón fibra corta y fotón por fibra larga.

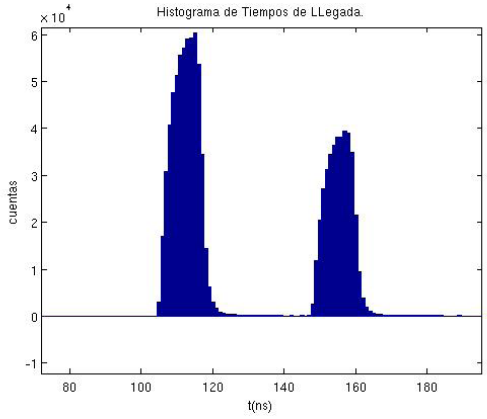


*Figura 7: Histograma de Tiempos de Llegada Relativos al Pulso de Encendido. El intervalo modal de la izquierda corresponde al evento fotón fibra corta y el de la derecha a fotón fibra larga.*

Para la extracción de bits de datos de llegada debemos definir los eventos 0 y 1 a partir del histograma. Para cada tiempo de llegada en la lista completa cuya distancia relativa en tiempo al último pulso de alimentación corresponde al intervalo modal de la izquierda (derecha) asignamos el evento 0 (1). El orden de los bits viene dado por el orden original de la lista de tiempos.

Para descartar las ocurrencias que corresponde al ruido propio del APD fijamos un criterio arbitrario de mínima frecuencia relativa

Si observamos la Figura 7 vemos que no es totalmente simétrico sino que esta sesgado hacia el evento 0. Esto implica que para los bits extraídos la probabilidad de ocurrencia $p$ del 0 será mayor a la probabilidad $q$ del 1. Esta situación se remedia a través de un algoritmo general que permite obtener, a partir de una fuente de bits 0 y 1 con probabilidades $p$ y $q$ dadas, una nueva sucesión de bits $\tilde{0}$ y $\tilde{1}$ tal que ambos tienen igual probabilidad de ocurrencia ( $\tilde{p} = \tilde{q} = 1/2$).

Este algoritmo fue desarrollado por J. von Neumann en 1951 [7] y la idea básica es la siguiente: a partir de las probabilidades de ocurrencia $p$ del 0 y $q$ del 1, y dada la independencia de la ocurrencia de cada uno, la probabilidad de obtener para dos bits consecutivos la

secuencia 01 es $\tilde{p} = p \cdot q$. De igual manera la probabilidad de ocurrencia de la secuencia 10 resulta ser $\tilde{q} = q \cdot p = p \cdot q = \tilde{p}$ .

El problema con el algoritmo de von Neumann es que se pierde buena parte de la información. Como respuesta a este problema Yuval Peres [8] diseñó un algoritmo de extracción que básicamente consiste en iterar el procedimiento de von Neumann para extraer bits de la porción de información que aquel descartaba. La eficiencia del procedimiento de Peres es mucho mayor que la de von Neumann, llegando en el límite a la entropía binaria de la secuencia original (que es $h(p,q) = -p\log_2(p) - q\log_2(q)$. Habiendo tomado el recaudo de alinear el sistema para lograr histogramas bastante simétricos ( $p \approx q$ ) el rendimiento del procedimiento de extracción fue bastante alto, en general cercano al 90% o más.

**B. Pruebas de aleatoriedad.**

Dada una fuente física de números pretendidamente al azar no existe a priori un argumento teórico que permita demostrar la verdadera naturaleza aleatoria o determinística de la misma. Lo que debemos hacer para comprobar la buena aleatoriedad de nuestra fuente es, en un enfoque probabilístico, considerar a las listas de bits obtenidas con nuestro generador como muestras de una población infinita compuesta por todos los posibles resultados de nuestra fuente.

Para poner a prueba la condición de bits al azar de las listas obtenidas se trabajó con una serie de pruebas correspondientes al grupo de *tests* de NIST [9] y algunas otras pruebas usuales en la literatura de generadores de bits al azar, como ser la correlación de bits a distancia *n* [5], el cálculo de π por el método de Monte-Carlo, las ocurrencias de bloques de n ceros o unos y la entropía binaria.

El resultado de las pruebas fue positivo para todas las series de bits balanceadas obtenidas, es decir que no revelaron ninguna desviación de la fuente respecto a la perfecta aleatoriedad. El valor empírico de los estadísticos de prueba fue en general << 0.01 para las series de más de 1 millón de bits.

En la Figura 8 se observa el resultado de la transformada de Fourier discreta para una serie balanceada de 925166 bits.

En la Figura 9 vemos el correlograma para la mencionada serie de 925166 bits y también la distribución normal de las correlaciones alrededor del valor medio.

Para la serie particular sobre la que presentamos resultados, con 925166 bits, la estimación fue π ≈ 3.12957. Este 0,38% de discrepancia es aceptado en la literatura [10] para este largo de serie.

Un cálculo también directamente relacionado con la proporción de ceros y unos en la muestra es la entropía binaria $h = -p \cdot log_2(p) - q \cdot log_2(q)$, que en este ejemplo es 0.99997114, extremadamente cercana a 1 (ideal).

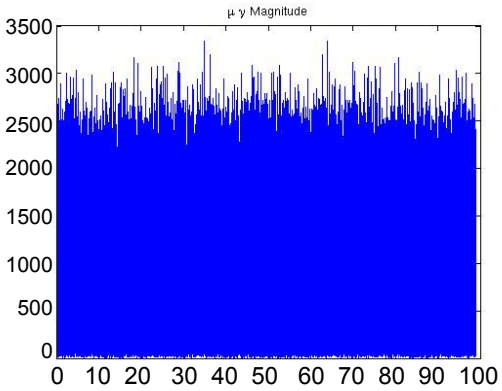


*Figura 8: FFT para una serie de 925166 bits. En todos los casos el examen espectral de Fourier descartó la existencia de patrones periódicos para un p-value p = 0.01.*

Por último es interesante estudiar la ocurrencia de bloques de 1's y 0's consecutivos. La distribución de bloques de n ceros y unos concatenados en una muestra debería ser proporcional a $2^{-n}$.

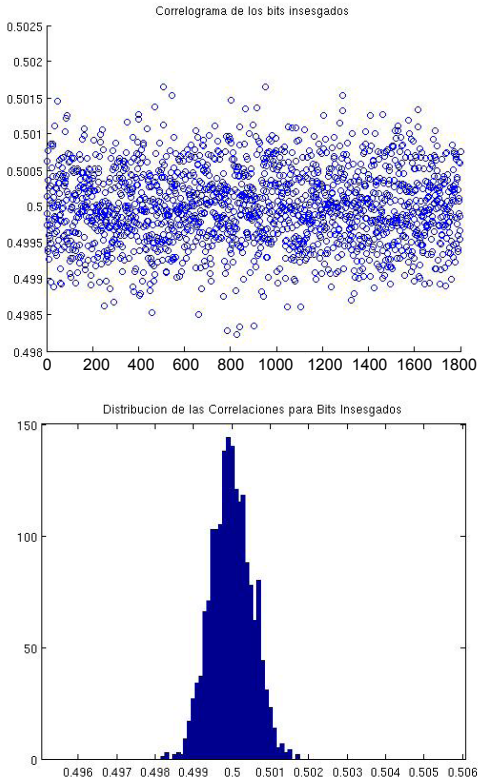


*Figura 9: Arriba: correlograma para una serie de 925166 bits. Abajo: las correlaciones se distribuyen normalmente alrededor de la media.*

En la Figura 10 se presenta un gráfico de las ocurrencias de bloque de n ceros o unos concatenados. Cuando se pasa a escala logarítmica la pendiente de las rectas debería ser, idealmente, −log 2 = −0.30103. En este ejemplo fueron -0.2891 y -0.2931, considerándose dentro de lo aceptable en experiencias similares [11].

**IV. CONCLUSIONES**

Desarrollamos una fuente física de números aleatorios basada en el comportamiento de un sistema óptico. El resultado se considera objetivamente aleatorio porque se fundamenta en la elección entre dos estados cuánticos puros que lleva a cabo un fotón que se encuentra inicialmente en la superposición coherente $\Psi = \alpha|0\rangle + \beta|1\rangle$.

Es importante señalar la sencillez del experimento comparado con otras posibles fuentes físicas, inclusive en aquellas basadas también en dispositivos ópticos, como ser los *beamsplitters* [12], *speckle* de láser, fotones de estados entrelazados [10], etc.

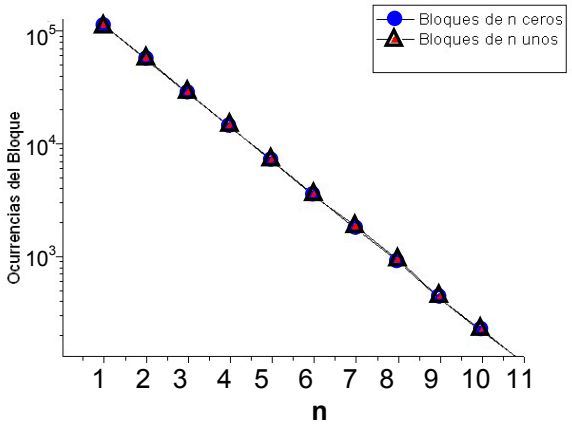


*Figura. 10: Ocurrencia de bloques de 1's (rojo) y 0's (azul) para el ejemplo de 925166 bits*

La versión automatizada del dispositivo nos permitió llevar la velocidad de obtención de bits a unos 25 kb/s, que resulta aceptable en comparación a otros tipos de generadores físicos [8]. Las series obtenidas superan todas las pruebas de aleatoriedad a las que fueron sometidas.

## V. REFERENCIAS


[1] W. Cochrane. Técnicas de Muestreo, CECSA (2000).

[2] P. L'Ecuyer, and P. Hellekalek, Random Numbers Generators: Selection Criteria and Testing, en Hellekalek & Larcher, Random and Quasi-Random Point Sets, Lecture Notes in Statistics **138**, Springer (1998).

[3] J. Lagarias. Statistical Science. Pseudorandom Numbers. **8**. pp. 31-39. (1993).

[4] A. Tonomura, J. Endo, T. Matsuda, T. Kawasaki and H. Ezawa, American Journal of Physics **57** pp. 117-120 (1989).

[5] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard and H. Zbinden, Journal of Modern Optics **47**, pp. 595-598 (2000).

[6] Los fotodiodos de avalancha tienen una probabilidad no nula (0.1% típicamente) de emitir un segundo pulso unos 100 ns después de la detección.

[7] J. Von Neumann, Applied Mathematics Series **12**, pp. 36-38 (1951).

[8] Y. Peres, The Annals of Statistics, **20** pp. 590-597. (1992).

[9] A. Rukhin, et al., A Statistical Test Suite for Random Number Generators for Cryptographic Applications, NIST Special Publication 800-22 (2001).

[10] M. A. Hai-Qiang et. al, Chinese Physics Letters **21**, p. 1961 (2004).

[11] T. Jennewein, et al., Review of Scientific Instruments **71**, pp. 1675-1680 (2000).

[12] M. Stipcevic,and B. Medved Rogina, Quantum Random Number Generator, arXiv:quant-ph/0609043v2 (2007).