Tema propuesto: Generación de números al azar basado en un láser caótico

Director: Dr. Marcelo G. Kovalsky* (Investigador Independiente, CONICET)
Co-directora: Dra. Mónica Agüero (Investigadora Asistente, CONICET)

Resumen
La propuesta se centra en la generación de aleatoriedad a partir de la salida de un láser caótico. La primera parte de la Tesis se dedicará a la construcción y caracterización de la fuente de entropía, un láser de estado totalmente sólido basado en Nd: YVO4 con comportamiento caótico. La segunda parte será la generación de las series aleatorias. Para ello se digitalizará la señal del láser, se realizarán operaciones lógicas y se emplearán test estadísticos y algorítmicos para verificar la aleatoriedad de las series generadas.

Lugar de trabajo: División Láseres Sólidos, CEILAP (Centro de Investigaciones en Láseres y Aplicaciones) (CITEDEF-CONICET), Juan B. de La Salle 4397, Villa Martelli. Tel.: 4709 - 8100 int. 1322.
Página web: www.lls-ceilap.com
***Contacto**: mkovalsky@citedef.gob.ar mgkovalsky@gmail.com

Objetivos

Se trata de un trabajo Teórico - Experimental, en el cual el estudiante adquirirá conocimientos sobre láseres, procesamiento de señales, y fundamentos de dinámica nolineal y mecánica cuántica.

Actividades que realizará el estudiante

En una primera etapa el estudiante se abocara al estudio de los fundamentos de los láseres sólidos y se familiarizará con las técnicas de diseño y alineación de cavidades láser [1]. Luego empleara estos conocimientos para la construcción y caracterización de un láser de estado totalmente sólido con comportamiento caótico. La etapa final de la tesis será la adquisición de series temporales del láser y, la aplicación de algoritmos para, a partir de éstas, generar cadenas de números aleatorios. Por otra parte se desarrollará software a partir de los conceptos de complejidad de Kolmogorov [2] y herramientas de análisis estadístico, para verificar el grado de aleatoriedad de las cadenas generadas.

Recursos materiales

Toda la óptica y la mecánica necesarias para la construcción del láser se hallan disponibles en el laboratorio. Asimismo el laboratorio dispone de lugar específico sobre una mesa óptica estabilizada para el desarrollo del trabajo. El laboratorio posee además osciloscopios de memoria adecuados para la obtención de series temporales.

Se dispone del apoyo técnico del taller de óptica del CEILAP, y de los talleres mecánicos del CEILAP y CITEDEF. El plan de trabajo de esta Tesis de Licenciatura se encuentra en el marco de los proyectos que están en curso en el Laboratorio, y cuenta con la financiación necesaria para ser desarrollados en tiempo y forma.

Antecedentes (breve descripción)

La necesidad de contar con cadenas de números al azar es cada vez mayor. A los campos tradicionales de aplicación, simulaciones numéricas, juegos de azar, pronósticos del clima o económicos, se suma el de la criptografía, dónde los números aleatorios tienen un rol crucial en la vulnerabilidad de las claves.

Los métodos para la generación de números aleatorios se dividen en dos, por un lado los basados en software para producir secuencias de números irregular, que aparentan ser aleatorios e impredecibles. Los números generados de esta forma son conocidos como pseudorandom. Dos sistemas que comiencen en el mismo estado inicial, generarán la misma secuencia. Para muchas aplicaciones, incluidas las simulaciones tipo MonteCarlo, esto es tolerable e incluso deseable. Sin embargo en aplicaciones de criptografía es intolerable. La ventaja de estos métodos es su simpleza y la posibilidad de alcanzar tasas de generación altísimas, su gran desventaja es que no son verdaderamente aleatorias. Como dijo J. Von Neumann [3] : “ Cualquiera que considere los métodos aritméticos de producir números aleatorios está, por supuesto, en un estado de pecado”.

La otra alternativa es generar una fuente de entropía física basadas en un fenómeno aleatorio (cuántico) o determinista pero muy sensible a condiciones iniciales como ruido térmico, tirar un dado o caos.

Si bien los sistemas cuánticos, en principio garantizan la aleatoriedad por el carácter cuántico del setup, su implementación es costosa y está limitada por la velocidad de los sistemas

detectores de fotones a unos 20 Mbit/s.

Una interesante alternativa surgió con los láseres caóticos, si bien el fenómeno es determinista, la extrema sensibilidad a condiciones iniciales, característica del caos, hace que sea impredecible mas allá de un horizonte calculable mediante los exponentes de Lyapunov. Con este tipo de sistemas es que se generan secuencias aleatorias a tasas del orden de los Gbit/s [4].

Información adicional

Duración: El plan de Trabajo está diseñado para que sea llevado a cabo en su totalidad en 2 cuatrimestres. Si el estudiante no adeuda más de dos exámenes finales es posible realizar la tesis en 6 meses.

Dedicación: 20 a 25 horas semanales.

Correlatividades: Las que figuran en la página de la materia. No se requiere conocimiento previo de conceptos de Dinámica no Lineal.

Otra información de interés: • El Instituto provee el almuerzo. • Existe la posibilidad de que el alumno se presente a una beca.

Referencias

[1] W. Koechner. *Solid-state laser engineering*. 6th edition, Springer, New York, USA (2006).

[2] A.Kolmogorov. *Three approaches to the quantitative definition of information*. Problems of Information Transmission, 1 p.4 (1965).

[3] von Neumann, J. J. Res. Natl Bur. Stand. Appl. Math. Ser. 12, 36-38 (1951); reprinted John von Neumann Collected Works Vol. 5 (ed. Taub, A. H.) 768-770 (New York, Macmillan, 1963).

[4] Uchida, A. et al. Nature Photon. 2, 728-732 (2008).