



Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Ref. Expte. N° 789/2021

Ciudad Autónoma de Buenos Aires, 31 de mayo de 2021

VISTO:

La nota presentada por la Dirección del Departamento de Computación, mediante la cual eleva la información del curso de posgrado **Curso intensivo en generadores cuánticos de números aleatorios** para el año 2021,

CONSIDERANDO:

lo actuado por la Comisión de Doctorado,
lo actuado por la Comisión de Posgrado,
lo actuado por este Cuerpo en la sesión realizada en el día de la fecha,
en uso de las atribuciones que le confiere el Artículo 113º del Estatuto Universitario,

**EL CONSEJO DIRECTIVO DE LA FACULTAD
DE CIENCIAS EXACTAS Y NATURALES
R E S U E L V E:**

ARTÍCULO 1º: Aprobar el nuevo curso de posgrado **Curso intensivo en generadores cuánticos de números aleatorios** de 15 horas de duración, que será dictado por el Dr. Gabriel Senno con la colaboración del Dr. Alejandro Díaz-Caro.

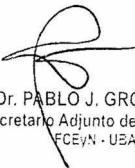
ARTÍCULO 2º: Aprobar el programa del curso de posgrado **Curso intensivo en generadores cuánticos de números aleatorios** para su dictado en julio de 2021.

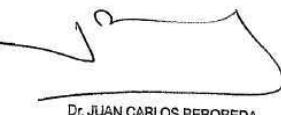
ARTÍCULO 3º: Aprobar un puntaje máximo de medio (0,5) punto para la Carrera del Doctorado.

ARTÍCULO 4º: Disponer que de no mediar modificaciones en el programa, la carga horaria y el arancel, el presente Curso de Posgrado tendrá una vigencia de cinco (5) años a partir de la fecha de la presente Resolución.

ARTÍCULO 5º: Comuníquese a todos los Departamentos Docentes, a la Dirección de Estudiantes y Graduados, a la Biblioteca de la FCEyN y a la Secretaría de Posgrado con copia del programa incluida. Cumplido, archívese.

RESOLUCIÓN CD N° 0752


Dr. PABLO J. GROISMAN
Secretario Adjunto de Posgrado
FCEyN - UBA


Dr. JUAN CARLOS REBOREDA
DECANO

Información académica

Año de presentación(*)

2021

1-a-

Departamento docente que inicia el trámite:
Computación
Nombre del curso:
Curso intensivo en generadores cuánticos de números aleatorios
Nombre, Cargo y Título del docente responsable:
Gabriel Senno, Profesor visitante, Doctor en Ciencias de la Computación de la Universidad de Buenos Aires.
Encasos dedicados para el desarrollo de la materia de grado, nombre de la misma:
Generadores cuánticos de números aleatorios
Nombre y Título de los docentes que colaboran con el dictado del curso (*) (*):
Alejandro Díaz-Caro. Doctor en Computación de la Université de Grenoble
Fecha propuesta para el primer dictado y luego de la aprobación:
Julio 2021 (ECI2021)

Duración:

Duración total en horas	15
Duración en semanas	1

Distribución carga horaria:

Número de horas de clases teóricas	10
Número de horas de clases de problemas	5
Número de horas de trabajos del laboratorio	
Número de horas de trabajo de campo	
Número de horas de seminarios	

Forma de evaluación:

Examen individual domiciliario.

Lugar propuesto para el dictado (departamento, laboratorio, campo, etc.):

Modalidad virtual

Puntaje propuesto para la carrera de doctorado:

0.5 puntos

Número de alumnos:	Mínimo: 5	Máximo: 50
Audencia a quién está dirigido el curso:		
Estudiantes de doctorado en Cs. de la Computación y especialidades afines.		

Necesidades materiales del curso:

Saladereunionesvirtual.

1-b-

Programa analítico del curso con Bibliografía (puede adjuntarse en hojas separadas):

La capacidad de generar números aleatorios es un recurso fundamental en informática, con importantes aplicaciones en simulación numérica y criptografía. El carácter inherentemente aleatorio del mecanismo cuántico convierte a los sistemas cuánticos en fuentes ideales de entropía.

En los últimos años, este hecho ha impulsado el desarrollo comercial de generadores cuánticos de números aleatorios (QRNG, por sus siglas en inglés) contribuyendo a su crecimiento basado en la (sólo) aparente aleatoriedad de ciertos sistemas clásicos (p. ej. caóticos). Más aún, el carácter local de las relaciones entre sistemas cuánticos entrelazados permite el diseño de QRNGs “independientes del dispositivo” (DI-QRNGs, por sus siglas en inglés) cuya salida se puede certificar independiente de la fuente que haya podido alterar el dispositivo de manera maliciosa.

En este curso estudiaremos los distintos protocolos para la generación cuántica de números aleatorios, yendo desde esquemas básicos detrás de los QRNGs hoy disponibles en la industria al diseño de DI-QRNG. Por último, discutiremos esquemas semi-DI que, acambio de relajar ligeramente las garantías de seguridad que se obtienen en los esquemas DI, permiten implementaciones más cercanas a las capacidades tecnológicas actuales.

Programa del curso:

- Extractores de aleatoriedad
- Generadores cuánticos de números aleatorios (QRNG)
- No-localidad de Bell
- Generación de aleatoriedad privada en esquema “independiente del dispositivo” (DI-QRNG)
- Unbalance entre garantías teóricas y facilidad de implementación: esquemas semi-DI

Programa de talladopordía:

- Lunes
 - Introducción al problema de la generación de números aleatorios
 - Entropía, entropía-mínima y fuentes débiles de entropía
 - Extracción de aleatoriedad
- Martes
 - Breve introducción al formalismo cuántico.
 - Primeras generaciones de generadores cuánticos de números aleatorios
- Miércoles
 - Generación de aleatoriedad en un esquema criptográfico (aleatoriedad privada)
 - No-localidad de Bell y esquema “independiente del dispositivo” (DI)

- Jueves
 - Amplificación y expansión de aleatoriedad privada en el esquema DI
 - Adversario cuántico vs. adversario clásico
 - La hipótesis IID (experimentos independientes idénticamente distribuidos)
- Viernes
 - Esquemas semi-DI para generación de aleatoriedad privada
 - Generación de aleatoriedad privada con una hipótesis sobre la energía media de los sistemas cuánticos

Bibliografía:

- Arora, S., & Barak, B. (2009). Computational complexity: a modern approach. Cambridge University Press, chap. 21.
- Herrero-Collantes, M., & García-Escartin, J.C. (2017). Quantum random number generators: views of Modern Physics, 89(1), 015004.
- Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V., & Wehner, S. (2014). Bell nonlocality. Reviews of Modern Physics, 86(2), 419.
- Acín, A., & Masanes, L. (2016). Certified randomness in quantum physics. Nature, 540(7632), 213-219.

Bibliografía Adicional:

- Nielsen, M.A., & Chuang, I.L. Quantum Computation and Quantum Information. Cambridge University Press, 2010. Capítulos 2, 9 y 11.
- Scarani, V. Bell nonlocality. Oxford University Press, 2019. Capítulos 2, 3 y 8
- Arnon-Friedman, R. Device-Independent Quantum Information Processing: A Simplified Analysis. Springer Nature, 2020. Capítulos 7 y 9.
- Arora, S., & Barak, B. Computational complexity: a modern approach. Cambridge University Press, 2019. Capítulo 21.

1-c-

Actividades prácticas propuestas (puede adjuntarse en hojas separadas):

(*) Todos los cursos tendrán una validez de 5 años

(*) (*) Las actualizaciones de los docentes colaboradores son informados por la Dirección departamental al inicio de cada dictadura del curso

Firma Subcomisión Doctorado

Firma del docente responsable

E-mail y teléfono del docente responsable

gsenno@gmail.com

+34 622346833

adiazcaro@icc.fcen.uba.ar

011 15 2889 1452

Solicitud de Financiación

Año de presentación(*)

2021

Departamento docente que inicia el trámite:

Nombre del curso:

Nombre y Título del docente responsable:

Costo propuesto del curso por alumno(*):

Justificación del monto propuesto:

(*) Las excepciones aplicables para cada alumno serán consistentes con la reglamentación del Consejo Directivo que regula las aranceles y excepciones (Res CD484/13). El docente responsable del curso solicitará las excepciones por nota al consejo directivo a través de MesadeEntradas.