

**Guía docente de la asignatura**

Asignatura	Temas de actualidad en Física Matemática		
Materia	Física		
Módulo	Especialización en FÍSICA MATEMÁTICA		
Titulación	Máster en Física		
Plan	617	Código	54441
Periodo de impartición	Segundo cuatrimestre	Tipo/Carácter	Optativa
Nivel/Ciclo	Máster	Curso	Primero
Créditos ECTS	3 ECTS		
Lengua en que se imparte	Español		
Profesor/es responsable/s	Juan Carlos García Escartín		
Datos de contacto (E-mail, teléfono...)	juagar@tel.uva.es		
Horario de tutorías	Véase la disponibilidad de cada profesor, o contáctese con él por correo electrónico.		
Departamento	Teoría de la Señal y Comunicaciones e Ingeniería Telemática		

1. Situación / Sentido de la Asignatura**1.1 Contextualización**

En esta asignatura se presentarán al alumno las herramientas matemáticas necesarias para entender las aplicaciones de la Física Cuántica a diferentes tareas de Computación y Comunicaciones. En concreto, se estudiarán las bases de las diferentes tecnologías basadas en la Información Cuántica como son la Criptografía Cuántica (distribución cuántica de claves), los generadores de números aleatorios cuánticos y las diferentes implementaciones de ordenadores cuánticos.

En la asignatura se pretende dar una visión actualizada de las tecnologías más avanzadas experimentalmente y de su posible impacto en computación y seguridad de las comunicaciones. En la mayoría de los protocolos prácticos, hay una etapa fundamental de procesamiento de los resultados experimentales que incluyen operaciones criptográficas (*hashing*, amplificación de la privacidad, ...) que deben relacionarse con los sistemas físicos utilizados para sacar el máximo partido a cada protocolo.

Se dará una perspectiva de las líneas de futuro más prometedoras y de la relevancia de las tecnologías actuales.

1.2 Relación con otras materias

Los contenidos de esta asignatura se complementan con los de la asignatura Información y Computación Cuánticas de éste Máster.



1.3 Prerrequisitos

Se intentará que la asignatura sea autocontenida suponiendo unos conocimientos generales coherentes con el acceso al Máster. En general son deseables, pero no imprescindibles, conocimientos de Óptica Cuántica, Álgebra Lineal, Teoría de la Probabilidad, Teoría de la Información y Teoría de Números. Para algunos de los ejercicios prácticos se recomienda experiencia en el manejo de algún lenguaje de programación científica.

2. Competencias

2.1 Básicas y Generales

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
- G1 - Capacidad de aplicación de conocimientos adquiridos: Capacidad para aplicar los conocimientos adquiridos y resolver problemas en entornos nuevos o poco conocidos dentro de contextos amplios y multidisciplinares relacionados con la Física.
- G2 - Capacidad crítica, de análisis y síntesis: Capacidad de integrar conocimientos y enfrentarse a la complejidad, de formular juicios a partir de una información incompleta o limitada.
- G4 - Capacidad de aprendizaje autónomo: Capacidad para continuar la formación de un modo autónomo, seleccionando de manera crítica las fuentes de información más pertinentes.

2.2 Específicas

- Comprensión de los distintos aspectos de Teoría de la Computación y Teoría de la Información relevantes en las tecnologías cuánticas.
- Comprensión de los aspectos prácticos más relevantes en la implementación práctica de los protocolos de Información Cuántica.
- Capacidad para identificar nuevos campos en los que la aplicación de los sistemas cuánticos pueda ser relevante.

3. Objetivos

- Entender la relevancia de las tecnologías cuánticas en problemas de computación y comunicaciones y su posible impacto en la sociedad.
- Comprender cómo deben tratarse los datos procedentes de los sistemas físicos para su uso en protocolos de Información Cuántica o en Criptografía.
- Entender las limitaciones prácticas de los sistemas actuales e identificar qué parámetros físicos son los más relevantes para que el sistema se aproxime a las suposiciones iniciales.
- Aprender a evaluar la calidad de los generadores de números aleatorios físicos.
- Aprender a identificar nuevas áreas de aplicación de las tecnologías cuánticas.



4. Contenidos

1. Implementación física de los ordenadores cuánticos. Sistemas actuales.
Criterios de implementación. Sistemas superconductores. Sistemas ópticos.
2. Ventaja cuántica. Muestreo bosónico.
Fundamentos de complejidad computacional. Complejidad de comunicación y juegos no-locales. Muestreo bosónico.
3. Generadores de números aleatorios cuánticos.
Números aleatorios y pseudoaleatorios. Aplicaciones en Ciencia y Criptografía. Generación de aleatoriedad a partir de sistemas físicos. Extracción y evaluación de la aleatoriedad.
4. Criptografía cuántica. Fundamentos matemáticos. Amplificación de la privacidad.
Canales autenticados: funciones Wegman-Carter. Amplificación de la privacidad. Información mutua. Sistemas independientes del dispositivo.
5. Evaluación de la seguridad. Implicaciones en criptografía.
Implicaciones de los algoritmos cuánticos en los sistemas actuales. Criptografía postcuántica.

5. Métodos docentes y principios metodológicos

Clase magistral participativa con resolución de problemas guiada. Ejemplos prácticos personalizados para el trabajo no presencial.

Se fomentará la participación del alumno y el uso de bibliografía científica (artículos en revistas). En la medida de lo posible, se propondrán ejercicios prácticos sencillos que ilustren los contenidos.

6. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teóricas	18	Asimilación de contenidos de las clases teóricas	18
Clases prácticas	6	Realización de problemas individualmente	15
		Realización de trabajos/entregas	18
Total presencial	24	Total no presencial	51



7. Sistema de calificaciones – Tabla resumen

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Resolución de problemas propuestos al alumnos de manera personalizada.	80-100%	
Exposición de la solución a los problemas propuestos o de un tema ante el resto de los alumnos.	0-20%	Dependiendo del número de alumnos se podrá pedir que se expongan en clase uno o varios de los ejercicios propuestos.
Examen escrito con problemas.	100%	Opcional. Lo podrán realizar los alumnos que deseen subir nota. 100 % de la nota para alumnos que decidan no realizar la evaluación continua.

CRITERIOS DE CALIFICACIÓN

Tanto para la convocatoria ordinaria como para la extraordinaria.

- Para los trabajos propuestos:
 - Profundidad en la comprensión del tema analizado.
 - Claridad en la explicación.
 - Capacidad de respuesta a las preguntas que se le formulan.
- Respecto del examen escrito:
 - Conocimiento de la materia expuesta durante el curso.
 - Capacidad de resolver problemas.
 - Capacidad de respuesta a las preguntas que se le formulan.

8. Bibliografía

Se proporcionarán artículos científicos sobre cada tema. Además, como bibliografía general se recomienda:

[1] M.A. Nielsen e I.L. Chuang, Quantum Computation and Quantum Information, Cambridge Univ. Press, 2000.

[2] N.D. Mermin, Quantum Computer Science: An Introduction, Cambridge University Press, 2007.

[3] Marcos Pérez-Suárez y David J. Santos, Procesado de información con sistemas cuánticos, Servicio de Publicaciones de la Universidad de Vigo, 2006.

9. Consideraciones finales

Este programa es orientativo. Dependiendo de la formación previa de los alumnos matriculados y los intereses que éstos expresen, los contenidos concretos podrán variar, previo acuerdo con los matriculados.