POLITÉCNICA
"Ingeniamos el futuro"

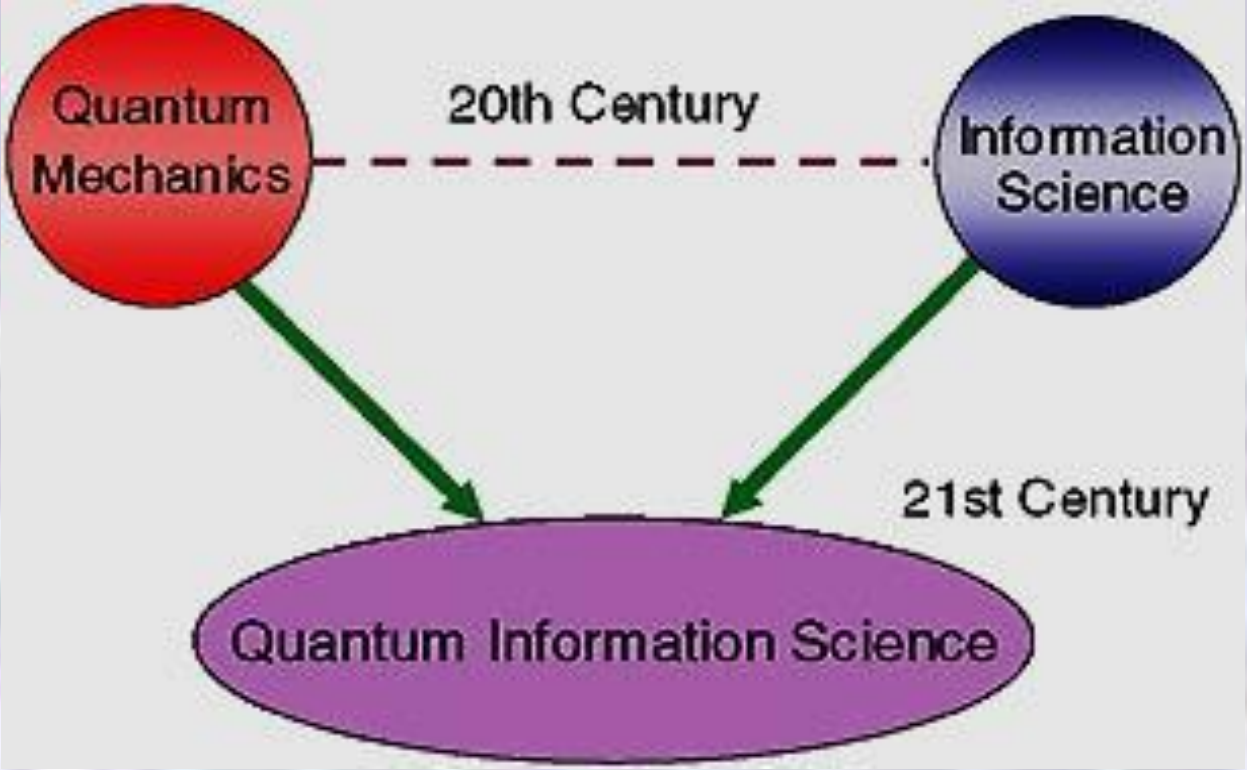
CAMPUS
DE EXCELENCIA
INTERNACIONAL

Introducción a la Información, Computación y Algorítmica Cuántica

Profesores Vidente Martin Ayuso
(Vicente@fi.upm.es)
José Luis Rosales Bejarano
(Jose.Rosales@fi.upm.es)

INFORMACIÓN CUÁNTICA

POLITÉCNICA
"Ingeniamos el futuro"
CAMPUS DE EXCELENCIA INTERNACIONAL



Objetivos del curso

- **Información y Computación Cuántica** desde un punto de vista de **Ciencias de la Computación**.
- La IC **permite resolver problemas que clásicamente** o bien **son imposibles**:
  - Transmisión de **claves con secreto garantizado**
  - **complejidad computacional menor** que la clásica Grover
  - **Cambiar de orden de complejidad** con respecto al mejor algoritmo clásico Algoritmo de Shor, que factoriza números en tiempo polinomial rompiendo sistemas de clave pública como RSA, Diffie-Hellman o curvas elípticas.
  - Resolver **problemas de optimización**, en farmacología, problemas de camino mínimo o para inteligencia artificial.
- Presente interés de Google, Microsoft o IBM.
- El curso acabará con una descripción de estos métodos y una breve descripción del hardware que se está usando para implementar los nuevos ordenadores cuánticos.

¿Qué es la computación cuántica?

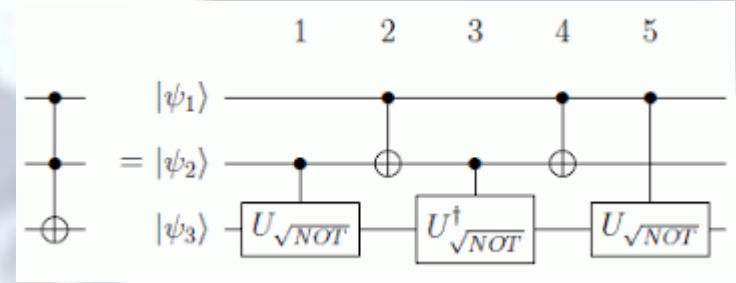
- Un nuevo modelo de computación basado en la mecánica cuántica
- Cada algoritmo equivale a un Hamiltoniano (un simulador cuántico)

$$i\partial_t|\psi\rangle = H|\psi\rangle$$

- Circuitos cuánticos, quantum Turing machines
- Más poderoso que los modelos de computación clásicos.

Algoritmos cuánticos

- Puertas lógicas cuánticas y circuitos cuánticos



- Factorización: dado N=pq, encontrar p y q.
- El mejor algoritmo clásico $2^{O(n^{1/3})}$, n –número de dígitos.
- $O(n^2)$ Algoritmo cuántico de Shor, 1994

Criptografía cuántica

- Distribución de claves: dos partes quieren crear una clave compartida secreta mediante el uso de un canal que se pueda escuchar a escondidas. [Bennett, Brassard, 1984].

Comunicación Cuántica

- Codificación densa: 1 bit cuántico puede codificar 2 bits clásicos.
- Teletransportación: los estados cuánticos se pueden transmitir enviando información clásica.

Qubits

- Estados de energía de un átomo o de un ón

ground state excited state

- Polarización de un fotón
- Estados cuánticos del flujo magnético en un circiuto LC superconductor

Base de la computación cuántica

- Un sistema cuántico k-dimensional quantum cuya base de estados es;
- $|1\rangle, |2\rangle, \ldots, |k\rangle$.
- Se puede preparar en cualquier combinación

$$\alpha_1|1\rangle+\alpha_2|2\rangle+\ldots+\alpha_k|k\rangle,$$

$$|\alpha_1|^2+\ldots+ |\alpha_k|^2=1$$

- El espacio posible de sus soluciones es 2^k correspondiente a un producto de k qubits

Operaciones lógicas posibles Ordenador Clásico vs. Cuántico

Clásico :

- se puede medir completamente,
- no se modifican con la medición,
- se puede copiar,
- se puede borrar.

Cuántico:

- se puede medir parcialmente,
- se cambian por medición,
- no se puede copiar,
- no se puede borrar.

Distribución de clave clásica vs cuántica

Clásicamente:

- Necesita supuestos matemáticos relativos a Hard-problems (imposible si el adversario tiene un poder computacional ilimitado.)

Cuánticamente:

- Los protocolos cuánticos pueden ser seguros contra cualquier adversario. El único supuesto: mecánica cuántica.

BB84 QKD

- **Alice envía n qubits**. Y **los mide con su propia base aleatoria**
- **Bob elige una nueva base aleatoria** cuya medidad coincidirá n/2 veces (cada elección tiene ½ de probabilidad de acertar en el bit medido por Alice)
- **Si no hubiera intrusos en la comunicación podrían compartir n/2 bits.**
- La **probabiliad de coincidencia** en la elección del bit (proyección de qubit) tomada al azar es $\mathbf{1/2^2 = 1/4}$
- Si después de medir Bob, este **comparte su base públicamente con Alice, descartaremos todos los bits que no se hayan obtenido con la misma base**
- **Reconiciliamos, compartimos k bits públicamente**, y vemos que la probabilidad de **no-error** del resto de nuestras medidas tiende a $1 - \left(1 - \frac{1}{4}\right)^k \to 1$

Prueba Cuántica de la existencia de un intruso

- Alice elige al azar una fracción de la cadena final y la anuncia.
- Bob cuenta el número de bits diferentes.
- Si hay demasiados bits diferentes, rechácelos (se encontró un espía).
- Si Eve midió muchos qubits, la atrapan.

Implmentaciones QKD

- First: Bennett et.al., 1992.
- En la actualidad: 67km, 1000 bits/second Madrid QCI Proyecto EU OpenQKD **En la UPM**
- Dispositivos comerciales disponibles en la actualidad: Id Quantique, Toshiba, Hw.

Temario

- 1. Conceptos fundamentales
  - 1.1. La información es física: qubits.
  - 1.2. Los fundamentos de la mecánica cuántica
  - 1.3. Computación cuántica
  - 1.4. Información cuántica
  - 1.5. Realizaciones experimentales de los conceptos y algoritmos fundamentales.

Temario

2 Criptografía cuántica

- 2.1. Ideas y algoritmos fundamentales en Criptografía Cuántica
- 2.2. Criptografía cuántica en la práctica.

Temario

- 3.Algoritmos fundamentales en Computación Cuántica
  - 3.1. Búsqueda Cuántica: Algoritmo de Grover.
  - 3.2. Factorización: Algoritmo de Shor.

Temario

- 4.Optimización Cuántica (trabajos de aplicación)
  - 4.1. Quantum annealing
  - 4.2. Aplicaciones.
- 5. Implementaciones físicas de la Computación Cuántica.
  - 5.1. Puertas básicas.
  - 5.2. Realizaciones del concepto de ordenador cuántico.

Temas

Conceptos fundamentales.
Criptografía cuántica.
Algoritmos fundamentales en Computación Cuántica (Shor + Grover)
Optimización Cuántica.
Implementaciones físicas de la Computación Cuántica.

- La documentación la tendreis disponible en Moodle (UPM/GATE)
  - Teneis ya un primer conjunto de documentos para empezar.
  - Advertencias: Teneis documentos muy diversos al que debereis dar un tratamiento diferenciado: desde atículos/charlas de divulgación hasta otros muy técnicos pasando por artículos fundacionales y transparencias de clase.

Evaluación:

- Evaluación Continua:
  - Supone una asistencia a un mínimo del 60% de clases.
  - El método de evaluación estará basado en la ejecución de dos proyectos durante el curso correspondientes, aproximadamente, a cada mitad del curso.
    - 1) Hasta Criptografía cuántica (aprox.)
    - 2) Desde Criptografía cuántica hasta fin de curso.
      - Nota: El tema de implementaciones físicas puede usarse tanto en el primero como en la segundo proyecto.
  - Cada proyecto consiste en el desarrollo y discusión de un tema asignado por grupos de un máximo de dos componentes.

Evaluación:

- Ambos proyecto tienen el mismo peso. Previamente a cada proyecto habrá una fase de definición del mismo en el que se discutirá el trabajo a realizar y se aceptará o no como tema válido.
  - El tema debe ser (preferiblemente, esto se evaluará positivamente) propuesto por el grupo.
  - La definición del proyecto consiste en la entrega de un escrito (dos páginas aprox.) especificando el tema, su objetivo, la razón por la que se propone e incluir un índice tentativo y una bibliografía básica.
  - Una vez propuesto y en el plazo de dos semanas, el grupo presentará un guión del trabajo (dos páginas indicando el índice previsto, principales ideas a desarrollar y bibliografía básica). Este guión será subido a Moodle y evaluado con un 10% de la puntuación de la parte correspondiente.

Evaluación:

- Durante las fechas esperadas (Semanas 8 y 16) el grupo realizará una exposición del trabajo (10-15 min.) ante la clase y atenderá sus preguntas.
- El material usado para la presentación así como cualquier otro material elaborado por el grupo y que éste considere necesario para su comprensión y correcta evaluación será subido (en un solo fichero) a la correspondiente entrega en Moodle.
- Las fechas esperadas para las presentaciones son:
  - Semana 8: Presentacion y desarrollo de los temas de discusión (Primera parte)
  - Semana 16: Presentacion y desarrollo de los temas de discusión (Segunda parte)

Evaluación:

- Evaluación única:
  - Siguiendo la normativa UPM, se admite el método de evaluación única mediante una prueba final para los que así lo deseen.
  - Debe solicitarse por escrito al coordinador de la asignatura en un plazo no superior a 30 días tras el inicio de las clases.
  - Consistirá en un examen de teoría y la solución de problemas propuestos. Se realizará en las fechas establecidas por jefatura de estudios.
- Examen Extraordinario de Julio: una
  - Examen del mismo tipo que la evaluación única. Se realizará en las fechas establecidas por jefatura de estudios.

Clases:

- Están distribuidas en clases de teoría (en general las clases de los miércoles) y clases marcadas como “actividades colaborativas” (en general las clases de los martes).
- El uso previsto de estas clases de actividades colaborativas es:
  - Discusión y asignación de los temas de los proyectos.
  - Clases adicionales/complementarias a las de teoría.
  - Conferencias especializadas.
  - Mini-cursos especializados: en particular, estamos intentando traer un curso específico para programación de ordenadores cuánticos.