UNIVERSIDAD SIMÓN BOLÍVAR
Vicerrectorado Académico

1 .Departamento: Física

2. Asignatura: **Información y Comunicación Cuántica Avanzada II**

3. Código de la asignatura: FS-7450

No. de unidades-créditos: 4

No. de horas semanales: Teoría 4 Práctica 2 Laboratorio 0

4. **Fecha de entrada en vigencia de este programa:** Enero 2017

5. Requisitos: Información y Comunicación Cuántica Avanzada I (FS-7449)

6. OBJETIVO **GENERAL:** Formar a los estudiantes con los conceptos y herramientas básicas necesarias para el estudio de las correlaciones cuánticas, así como sus aplicaciones en Computación Cuántica, Circuitos Cuánticos, Algoritmos Cuánticos y Criptografía Cuántica.

7. (Opcional) **OBJETIVOS ESPECÍFICOS:** El estudiante tendrá competencias para:

1.-Manejar fluidamente los conceptos relacionados con las correlaciones cuánticas que van más allá del entrelazamiento cuántico, y su dependencia del flujo de información inaccesible.
2.- Entender y desarrollar operativamente circuitos cuánticos.
3.- Entender y desarrollar algoritmos cuánticos fundamentales, así como su representación usando circuitos cuánticos.
4.- Entender los fundamentos básicos físicos y matemáticos de la criptografía cuántica.
5.-Dominar algunos de los protocolos de uso más común en criptografía cuántica, considerando estados discretos y/o continuos, y usando estados productos o entrelazados.
6.- Simular algunos protocolos de criptografía cuántica usando un computador convencional.
7.-Dominar los conceptos básicos de la teoría de corrección de errores cuánticos, su representación circuital y su implementación en la computación cuántica basada en medidas.

8. CONTENIDOS**:**

1.- CORRELACIONES CUANTICAS: Fundamentos y Propiedades. Correlaciones cuánticas más importantes:

1.a) Definición de discordia cuántica: Propiedades, implicaciones e importancia. Aplicaciones a la computación cuántica. Caso bipartito y multipartito. Discordia Cuántica Global.

1.b) El déficit cuántico.

1.c) La medida geométrica de la discordia cuántica para sistemas de dos-qubits: Definición y aplicaciones relevantes.

1.d) Coherencia Cuántica: Propiedades de la coherencia cuántica y definiciones. Aplicaciones.

1.e) Flujo de Información Cuántica Inaccesible.

2.- ELEMENTOS DE COMPUTACION CUÁNTICA: Correspondencia entre compuertas clásicas y compuertas cuánticas. Compuertas cuánticas de un qubit, compuertas controladas y generación de entrelazamiento, compuertas cuánticas universales**.** Teorema de la no-clonación y su relación con las compuertas cuánticas. Circuitos de Codificación densa y Teleportación. Modelos alternativos.

3.- ALGORITMOS CUANTICOS: Algoritmo de Deutsch. Algoritmo de Simon. Algoritmo de Deutsch-Jozsa. Transformada Cuántica de Fourier y representación circuital. Algoritmo de búsqueda de Grover. Algoritmo de factorización de Short. Algoritmo de Bernstein-Varizani.

4.- PROTOCOLES DE CRIPTOGRAFÍA CUÁNTICA: Introducción a la Criptografía Clásica. Fundamentos de la Criptografía Cuántica. Alfabeto cuántico.

4.1.- **DISTRIBUCION DE LLAVES CUANTICAS (QKD):** Cifrado y distribución de claves. Distribución de claves cuánticas públicas y privadas. Teoría de la información y reconciliación de claves. Distribución de llaves en variable continúa con entrelazamiento en el medio. Distribución de llaves cuánticas con sistemas bipartitos y tripartitos de estados coherentes. vAnálisis de seguridad (ataques y vulnerabilidad). Redes de distribución cuántica de llaves. Autenticación y certificación.

4.2.- **Protocolos basados en conjuntos de estados ortogonales:** BB84, B92, Estados trampa, SARG04, Ping-pong, estados decodificados, DPS, COW, S09 y S13.

4.3.- **Protocolos basados en estados entrelazados**: E91, protocolos cuánticos de comparación privada usando estados y medidas de Bell. Protocolo de acuerdo de llave cuántica con estados clúster.

4.4.- **Protocolos con variables continuas**: Protocolos con estados coherentes bipartitos (GC02) y tripartitos. Protocolos con entrelazamiento y empate en el medio.

Análisis de QKD en sistemas de fibras ópticas y en la transmisión de información en espacios libres a largas distancias. Ilustrar las aplicaciones de estas nuevas tecnologías.**:** Aplicaciones a sistemas de transmisión de data en procesos electorales, seguridad aeronáutica, seguridad industrial y militar, comunicaciones satelitales, etc.

5) CORRECCION DE ERRORES CUANTICOS: Corrección clásica y cuántica de errores. Código cuántico de tres qubit para el error Bit-Flip y el Phase-Flip. Discretización de errores. Códigos estabilizadores de corrección cuántica de errores. Algoritmo de Shor a cinco, a siete y a nueve qudits. Computación cuántica basada en medidas. Computación cuántica en una dirección.

9. ESTRATEGIAS METODOLÓGICAS, DIDACTICAS O DE DESARROLLO DE LA ASIGNATURA.

Se recomiendan las siguientes:

1. Clases magistrales
2. Sesiones de Ejercicios y/o Problemas
3. Talleres
4. Seminarios
5. Investigaciones
6. Presentaciones
7. Simulaciones computarizadas

10. ESTRATEGIAS DE EVALUACIÓN.

Se recomiendan las siguientes:

1. Pruebas escritas y/o verbales
2. Informes de simulaciones de protocolos y su transmisión por redes cuánticas
3. Ejercicios, tareas y/o asignaciones para realizar fuera del aula.
4. Búsqueda de publicaciones científicas e ingenieriles, relevantes y novedosas en el área de la criptografía cuántica, así como una explicación completa y detallada, del contenido de las mismas, en exposiciones orales y/o escritas.
5. Investigación de problemas específicos, y la formulación de propuestas para resolverlos usando los conocimientos aprendidos en el curso.

11. FUENTES DE INFORMACIÓN:

1.- Masahito Hayashi, Satoshi Ishizaka, Akinori Kawachi, Gen Kimura, Tomohiro Ogawa, "Introduction to Quantum Information Science", Springer-Verlag Berlin Heidelberg, (2015)

2.- Alexander Streltsov, "Quantum Correlations Beyond Entanglement and Their Role in Quantum Information Theory ", Springer (2015)

3.- Sandor Imre and Laszlo Gyongyosi "ADVANCED QUANTUM COMMUNICATIONS: An Engineering Approach", John Wiley and Sons, INC., Publication, (2013)

4.- R. J. Lipton and K. W. Regan "QUANTUM ALGORITHMS VIA LINEAR ALGEBRA: A Primer", Massachusetts Institute of Technology (2014)

5.- Song Y. Yan, "Quantum Attacks on Public-Key Cryptosystems", Springer New York Heidelberg Dordrecht London. (2013)

4.- Mark M. Wilde, "Quantum Information Theory", McGill University, Montréal (2013)

7.- Christian Kollmitzer y Mario Pirk, "Applied Quantum Cryptography", Springer-Verlag, Berlin Heidelberg, (2010)

8.- Daniel J. Rogers, "Broadband Quantum Cryptography", Morgan and Claypool Publishers, (2010).

9.- M. A. Nielsen y I. L. Chuang, "Quantum computation and quantum information", Cambridge University Press, (2010)

10.- Mikio Nakahara and Tetsuo Ohmi, "Quantum Computing, from Linear Algebra to Physical Realizations". CRC Express. (2008)