Universidad Latinoamericana de Ciencia y Tecnología

Facultad de Ingeniería

Escuela de Ingeniería Informática

Trabajo Final para optar por el Grado de Licenciatura en Informática con Énfasis en Telemática y Redes

Tema

Mecánica Cuántica aplicada a la Informática

Sustentante: Jorge Rojas Rodríguez

Cédula: 205810471

Tutor: Lic. Miguel Pérez Montero

III Cuatrimestre 2009

Índice.

El mundo cuántico: Principios de Mecánica Cuántica aplicados a la Informática.

Jorge Rojas Rodríguez.
Bachiller en Ingeniería Informática.
Candidato a Licenciatura en Ingeniería Informática con Énfasis en Redes y Sistemas Telemáticos, ULACIT.
Correo Electrónico: jorgemiguelcr@gmail.com

"If you think you understand quantum mechanics, you don't understand quantum mechanics"
(Ball, 2001)

Resumen.

La mecánica cuántica ha llegado a cambiar radicalmente la aplicación de los principios de física clásica aplicados al mundo macroscópico para de esta forma, explicar la interacción de las partículas a nivel microscópico. Esto debido a que a nivel atómico suceden distintos fenómenos que no pueden ser reducidos a pensar en términos de la física newtoniana.

Características como *causalidad, objetividad, determinismo, no localidad y completez* sustentan a nuevas técnicas para innovar las tecnologías de información como el procesamiento de datos, desarrollo de algoritmos eficientes bajo conceptos cuánticos como superposición, la teleportación y encriptación cuántica, por citar algunos campos.

Una de las características que diferencian los procedimientos cuánticos para tratar los datos es el uso de qubits: como unidades, pueden tomar los valores de un bit clásico (0 o 1) o una combinación de ambos debido a la capacidad de superposición.

La medición de las propiedades de las partículas no permite modificar todo el sistema, por lo que han tenido que utilizarse métodos probabilísticos para encontrar la posición y desplazamiento y así conocer su estado. Actualmente por medio de filtros y mediciones del spin de las partículas mediante el uso de vectores, es que se pueden llevar a la práctica algunas aplicaciones como la criptografía. Esto no implica la inexistencia de errores, pero conforme pasan los días se encuentran nuevas formas de corrección de errores.

El entrelazamiento cuántico de partículas provee un gran abanico de innovaciones. Sin embargo, hasta el momento la mayoría han sido llevadas a cabo en la teoría, pero se han dado pocas demostraciones en laboratorio. Por lo tanto, este artículo pretende dar una visión global de la teoría e implementación de principios cuánticos en el campo de la informática. Así mismo se intenta despertar el interés y la imaginación para la concepción de nuevas ideas tomando como base la teoría cuántica.

Abstract.

Quantum mechanics has come to reverse the application of the principles of classical physics applied to the macroscopic world to explain the interaction that occurs with microscopic particles or atomic level. This is because at the atomic level very different things happen that can't be reduced to Newtonian physics conclusions. Features such as causality, objectivity, determinism, locality and completeness are some that support to innovate new techniques to processes involving information technology and data processing, development of efficient algorithms under concepts such as quantum superposition, teleportation and quantum encryption, to name a few fields.

One of the distinguishing features of quantum processes to treat the data with respect to the classical way is the use of qubits as units that can take the values of a classical bit (0 or 1) and also a combination of both because superposition ability.

Measuring the properties of the particles is impossible to avoid the whole system doesn't change, so have had to use probabilistic methods to find the position and movement to track their status. Currently through filters and measurement of the spin of particles involving the use of vectors, is that you can implement some applications like cryptography. This does not imply the absence of errors, but as the days go find new ways of correcting errors.

The particle quantum entanglement provides a range of innovations that so far most have been conducted in very small theory and laboratory demonstrations. Therefore this article attempts to provide an overview from theory to implementation of principles in the field of quantum computing, implicitly claiming to arouse the interest and imagination to the conception of new ideas based on quantum theory.

Lista de Palabras Clave.

Qubits, Mecánica cuántica, dualidad onda-partícula, informática cuántica, entrelazamiento cuántico, teleportación.

Introducción.

Durante los últimos años, una de las principales tendencias de la investigación ha sido el desarrollo de lo que bien se podría llamar “Ingeniería Cuántica”. Esta consiste en la manipulación o tratamiento de la materia a escalas extremadamente pequeñas con el fin de modificar sus propiedades cuánticas fundamentales. Una de las ramas que se encargan de estudiar la interacción de estos elementos de la materia y sus propiedades es la mecánica cuántica, conocida también como mecánica ondulatoria. La mecánica cuántica ha roto con cualquier paradigma de la física hasta este momento: con ella se ha descubierto que el mundo atómico no se comporta como esperaríamos. *Incertidumbre, indeterminación o cuantización* han sido conceptos introducidos por primera vez en este campo.

La reducción de los componentes electrónicos que usa la tecnología del mercado actual parece estar llegando a su límite. Esto hace difícil continuar con esta “miniaturización”, por lo que pronto se espera llegar a alcanzar los niveles de moléculas o componentes de los átomos a nivel individual, si tomamos en consideración la Ley de Moore. Al mismo, tiempo se hace necesario tocar el campo de la mecánica cuántica, donde operan leyes físicas diferentes a las que conocemos como las que rigen la vida cotidiana de la naturaleza a escala macroscópica, o sea, conforme a las leyes físicas convencionales aprendidas desde el colegio. Sin embargo, no hay razones en virtud de las cuales el comportamiento del mundo atómico y subatómico deba seguir las mismas pautas que los objetos de nuestra experiencia diaria.

El progreso de los principios e ideas básicas de la mecánica cuántica comenzó a inicios del siglo anterior: una serie de observaciones y descubrimientos pusieron al descubierto las dificultades de la física clásica para interpretar las propiedades del átomo y las partes que lo constituyen, al igual que las propiedades de la radiación electromagnética y su interaccionar con la materia. Estos descubrimientos dieron paso a una revolución de las nociones hasta entonces sustentadas por los físicos y plantearon una gran cantidad de incógnitas, cuya solución los obligó a realizar un profundo replanteo de los conceptos y fundamentos básicos de la física.

A pesar de que sus fundamentos involucran aspectos que aún no han sido aclarados de manera completamente satisfactoria; estos son la herramienta teórica básica para disciplinas muy importantes como la Física de la Materia Condensada, Química Física, Física de Partículas y la Física Molecular, Atómica y Nuclear.

Una característica que diferencia la Mecánica Cuántica de la Clásica, es que por razones de principio, resulta imposible efectuar una medición sobre un sistema sin perturbarlo. Motivos como estos fueron los que hicieron a los científicos más brillantes del siglo XX a estudiar a fondo la Mecánica Cuántica, donde en el presente artículo se describirán sus teorías y experimentos, así como su evolución a través del tiempo.

El proceso cuántico de la información es una de las áreas que hace uso de esta maravillosa ciencia y se destaca por ser reciente, multidisciplinaria y muy dinámica. Desde el punto de vista de sus aplicaciones se pueden distinguir algunas de gran envergadura como: procesamiento algorítmico de la información, simulación eficiente de sistemas cuánticos (dispositivos nanotecnológicos o microelectrónicos, moléculas) y comunicaciones seguras basadas en la distribución cuántica de claves. La primera aplicación mencionada potencia la realización de tareas relevantes de forma mucho más rápida que una computadora clásica. El tema convoca a especialistas de diferentes disciplinas (como las citadas líneas atrás) y de otras áreas de conocimiento, pues existe una sinergia entre los desarrollos teóricos y los avances experimentales que permiten implementarlos.

La falta de algoritmos que en situaciones de importancia práctica aprovechen la ventaja cuántica es una de las carencias más críticas. Sin embargo los procesos markovianos han servido como base para la gran variedad de algoritmos estocásticos (Motwani y Raghavan, 1996).

Entre los grandes desafíos de la Física a corto plazo está el desarrollo de la Información Cuántica en sus dos ramas principales: Computación Cuántica y Comunicación Cuántica. Esta última se trata de "Criptografía Cuántica", que está gestando un cambio cualitativo fundamental en la tecnología de las comunicaciones. Al utilizarse los principios cuánticos empieza a ser posible la transmisión codificada de información de forma supersegura, de manera que un mensaje no puede ser leído por nadie o en caso de que alguien llegara a leerlo el destinatario se aperciba de eso. Esto es un evolución muy notable ya que en la comunicación convencional es posible leer un mensaje sin que nadie se de cuenta.

El fin de este documento es explicar en qué consisten los principios cuánticos que, como dijimos anteriormente, no son completamente compatibles con las leyes de la física clásica y sus conceptos newtonianos. Además, como punto más importante, conocer su aplicación al campo de las ciencias de la informática y comunicación, para lo cual es sumamente necesario tratar de entender principios diferentes a los que rigen los elementos macroscópicos de la vida cotidiana. Con ello no se pretende explicar en detalle, a nivel subatómico, los teoremas y enunciados que han desarrollado los científicos en cada uno de sus experimentos; pero sí exponer de manera general a la comunidad de informáticos cada uno de los temas por desarrollar en la jerga del gremio.

Ojalá el artículo despierte el interés en el gremio no solo de informáticos (los cuales nunca llevamos cursos de física en la universidad, y por tanto, el entendimiento es más complicado), sino también en las carreras de mecánica, electrónica, industrial o cualquiera que tenga que relacionarse con aspectos del mundo atómico y su inesperado e impredecible comportamiento estocástico en el ámbito cuántico.

Historia de la Mecánica Cuántica.

La naturaleza de la luz ha sido impugnada a través de la historia de la ciencia moderna. Robert Hooke y Christian Huygens comenzaron a trabajar en una teoría ondulatoria de la luz en la década de 1670. Esta dependía de la idea de que las ondas de luz se propagan a través de un medio, por lo que el vacío entre el Sol y la Tierra debía estar lleno de "*un éter*".

En 1704 Newton propuso una teoría corpuscular (formada de partículas) de la luz y presentó resultados experimentales para probar su teoría. Esta fue controversial debido a que Newton tenía que usar cualidades ondulatorias para poder explicar el fenómeno de la difracción. La Teoría corpuscular de Newton sugirió que la luz podría viajar más rápido en un medio más denso, lo que fue negado por la teoría ondulatoria de la luz. Por supuesto, esto solo era posible verificando experimentalmente los resultados de Newton. No fue posible realizar estos experimentos sino hasta 1850 y los resultados de Foucault demostraron lo equivocado de Newton. Thomas Young y Augustin-Jean Fresnel ya habían aportado pruebas experimentales en favor de la teoría ondulatoria de la luz a comienzos del siglo XIX. Sus famosos experimentos de doble rendija mostraron que la luz producía patrones de interferencia de las ondas y Young pasó a explicar los resultados de Newton en términos de teoría de ondas.

Hacia el final de la década de 1800 Maxwell propuso que la luz puede entenderse como la propagación de las ondas electromagnéticas: en cualquier punto de un haz de luz hay una fuerza eléctrica y una fuerza magnética moviéndose perpendicularmente unas con otras en la dirección del haz de propagación. Estos campos de fuerza oscilan periódicamente y por lo tanto son detectados como ondas. Maxwell demostró esto al verificar un conjunto de cuatro ecuaciones que describen la interrelación entre el campo eléctrico, campo magnético, la carga eléctrica y la corriente eléctrica.

Max Plank introdujo por primera vez el concepto de quantum en 1900 y esto volvió a meter la teoría corpuscular de la luz. Plank estaba mirando la relación entre la cantidad de radiación que emite una de cuerpo negro y su temperatura y encontró que los datos experimentales sólo tenían sentido si se supone que irradia energía en discretos "quantums" o fotones, cada uno con un paquete de energía proporcional a la frecuencia con que se irradian. Esta constante de proporcionalidad es conocida como la constante de Plank.

De la constante de Plank se desprendieron muchas teorías y teoremas que se desarrollaran mas adelante con mayor detalle. Sintetizando la historia, William Thompson, conocido posteriormente como Lord Kelvin, fue el físico más notable a finales del siglo XIX en Inglaterra. En 1890, había declarado en una conferencia que se habían descifrado todos los misterios del mundo material y que solo dos pequeñas nebulosas quedaban pendientes de resolver por los físicos. Este destacado físico hacía el llamado a los estudiantes graduados en física para que buscaran otros campos del conocimiento, puesto que en su ciencia de estudio no quedaba casi nada por hacer (Kafatos y Nadeau, 1999).

Las incógnitas pendientes por resolver eran: el resultado fallido de los experimentos de Morley y Michelson para encontrar el éter luminífero y la “Catástrofe del Ultravioleta”, sinónimo que se le dio al problema de la radiación de cuerpo negro. Este último se refería principalmente al cálculo de radiación que emite un cuerpo caliente. Los resultados teóricos llevaban a cantidades infinitas para la energía total de radiación, resultado inaceptable por supuesto para cualquier teoría física.

Estas dos incógnitas o nebulosas que parecían a simple vista pequeñas para muchos físicos, llevaron a las dos grandes revoluciones en la física del siglo XX: La teoría de la mecánica cuántica y la de la relatividad, las cuales se generaron, por el problema de la radiación del cuerpo negro y por el experimento de Morley y Michelson.

En la evolución de la física, cuando los instrumentos y herramientas de medición alcanzaron la precisión para llegar a hacer observaciones a nivel atómico, se descubrió que la descripción de los diversos fenómenos asociados con las leyes físicas que se utilizaban en el año 1900, y que hoy se conocen como “física clásica”, nos llevaban a resultados que no coincidían con los experimentos o nos daban resultados absurdos. Este suceso llevó a la elaboración de una nueva teoría para tratar de explicar los fenómenos del mundo atómico. Esta teoría de mecánica cuántica fue desarrollada entre 1924 y 1927 por muchos físicos pero entre los más destacados estuvieron Paul M. Dirac, Werner Heisenberg y el físico Austriaco Erwin Schrodinger.

Diferente de teorías clásicas como el electromagnetismo o la mecánica, en las que se puede predecir con absoluta precisión cuál sería el resultado de la medición de una cantidad física, en la mecánica cuántica esto no suele ocurrir. La posibilidad de predicción es algo que caracteriza la teoría clásica: poder calcular o predecir cuánto tardará un objeto en caer al suelo, donde caerá y cuál sería su trayectoria, por citar un ejemplo, son aspectos que le dan valor y hacen confiable una teoría acerca del dinamismo de una partícula en el campo gravitacional del planeta Tierra. Una teoría como esta, con esa singularidad, se dice que es *determinista*, es decir, aquella donde se conocen las condiciones iniciales de un sistema y donde se puede predecir cómo evolucionará la misma en el futuro.

En la mecánica cuántica (M.C.) no es posible predecir el resultado de la medición de una cantidad física, únicamente se puede hacer referencia a la probabilidad de obtener un determinado valor lo cual convierte a la M.C. en una teoría *no determinista*. Al inicio, muchos físicos se vieron molestos, entre ellos Einstein, quién dijo estar en desacuerdo con la mecánica cuántica y lo expresó a través de una famosa frase: "Dios no juega a los dados" (Mackey, 1963), ya que estaba de parte del principio de casualidad, y por lo tanto, del determinismo. No aceptaba la probabilidad como algo válido para el uso en las teorías. Lo irónico es que aunque Einstein había dicho que el sentido común era el conjunto de prejuicios que se formaban en el individuo antes de los 18 años y que además él era quién había revolucionado la física con teorías propias como la general, especial y relativista, en esta parte de la historia mostraba una postura incongruente con sus principios al rechazar la mecánica

cuántica, que rompía con el prejuicio del determinismo al ser una teoría revolucionaria. Por cierto, a esta frase Neils Borh le respondió diciéndole “Quién es usted para decirle a Dios que hacer” (Mackey, 1963).

La M.C. incorporó conceptos totalmente nuevos en la física. Un principio como el de incertidumbre de Heisenberg donde rechazaba el determinismo, nos llevó a una nueva perspectiva de la realidad. La forma en que la naturaleza en su escala atómica se comporta, confronta, radicalmente los esquemas o estructuras mentales forjadas en la física clásica. Sin embargo, esta teoría recibió la aprobación de gran cantidad de físicos debido a la concordancia de predicciones cuantitativas con resultados experimentales y el éxito de la teoría para explicar los fenómenos observados.

Un vistazo a los principios de la mecánica cuántica.

Aun con el conocimiento y evolución de la historia de la mecánica cuántica, puede ser de más fácil absorción a lo largo de este artículo familiarizarse con algunos conceptos clave que facilitan captar su esencia en su nivel más fundamental:

- La dualidad *onda-partícula*. Isaac Newton teorizó que la luz estaba formada por partículas. En el siglo XIX Thomas Young anuló esta teoría al creer que la luz consistía de ondas. Con el inicio de la mecánica cuántica, quedó claro que la luz consiste, curiosamente, de ambas.

- La observación de que la luz existe en forma de partículas es donde el término "quantums" viene. Las partículas de luz son conocidas como "quantums" de luz, que son las más pequeñas porciones de energía que pueden existir. Con esta teoría finalmente se vino a aclarar la relación entre el color de la luz y la emisión de radiación.

- Estas partículas se mueven en un patrón de onda, lo que explica los resultados experimentales de Thomas Young, quien llegó a la conclusión de que la luz se comporta como una onda. Sin embargo, según la mecánica cuántica, estas ondas no son efectivas con respecto a las ondas de física comunes, pero las ondas de probabilidad definen las posibilidades de encontrar cada uno de los quantums individuales (o "fotón", como se denomina más comúnmente) en cualquier momento dado.

- El principio de incertidumbre de Heisenberg. Define que en un "fotón" no se puede observar ni una partícula y una onda al mismo tiempo cuando se someten a medición. En otras palabras, las cualidades de "onda" (que definen el impulso de la partícula) y las cualidades de "partícula" (que definen la posición exacta de la partícula) no pueden ser conocidas al mismo tiempo. Así, se puede medir ya sea la posición de un fotón, o su impulso, pero nunca ambos. De esta forma, cada fotón individual es más o menos imposible de definir por completo (por lo tanto, la incertidumbre).

- Cualquiera de estos cuatro primeros puntos son válidos no sólo para el electromagnetismo (luz y la energía), sino también para todos los objetos. Sin embargo, estas propiedades de la mecánica cuántica sólo son medibles cuando se trata con partículas subatómicas de manera individual. Conforme los objetos se hacen más grandes, las propiedades de la mecánica cuántica disminuyen rápidamente. Por lo tanto, en cualquier objeto visible, cada átomo individual puede ser imposible de definir y sería como una entidad colectiva que obedece las leyes estadísticas, por lo que son predecibles y tangibles.

Teorías de la física clásica.

Desde la perspectiva clásica de las teorías, si esta es científica debería ser *causal, objetiva, determinista, local y completa*. La objetividad se refiere que la naturaleza es independiente de nuestra percepción o conciencia, y el resultado de una medición u observación no dependen del observador.

En física, la causalidad detalla la relación entre causa y efecto. Este principio establece que vistas determinadas circunstancias siempre deben generarse los mismos efectos o resultados; por ende, se dice, según los principios de la teoría causal, que a una determinada causa le corresponde un efecto único. No obstante, a principios de este siglo Heisenberg introdujo su "principio de incertidumbre", que modificaba profundamente el principio de causalidad clásico. En cuanto al determinismo, consiste en que partiendo de un estado dado, se puede predecir y definir unívocamente cualquier estado posterior del mismo sistema (Morrones, 2005).

La localidad en palabras de Einstein (1948) significa que: *"la siguiente idea caracteriza la independencia relativa de objetos que están muy alejados uno de otro en el espacio (A y B): una influencia externa en A no puede influir directamente sobre B; esto es conocido como el principio de acción local, y es empleado una y otra vez en teoría de campos. Si suprimiéramos por completo este axioma, resultaría inviable la idea de la existencia de sistemas semicerrados, y no podríamos postular leyes que se pudieran comprobar experimentalmente en el sentido aceptado"*. En otras palabras, un acontecimiento físico no puede perturbar otro acontecimiento con el que no exista una conexión causal, o bien dos objetos lo suficientemente alejados uno de otro no pueden interactuar, de manera que cada objeto sólo puede ser influido por su entorno inmediato. Por ejemplo, el impacto de las dos naves de la misión LCROSS contra la luna el 09 de octubre del 2009 no puede afectar un sistema en la tierra debido a su entorno (NASA, 2009). En caso de que existiera una conexión de causalidad, el efecto solo podría afectar el sistema después de que la señal llegara hasta él; en este caso hipotético, un segundo que es lo que tardaría en llegar la señal de la luna a la tierra.

Por último, para que una teoría científica sea completa es necesario que a cada elemento o variable de la teoría física le corresponda un elemento de realidad física que sea medible con precisión absoluta en un sistema y que esta medición se pueda efectuar sin alterar el sistema.

La Mecánica Cuántica.

El mundo atómico junto con sus partículas elementales se comporta de manera muy distinta al mundo de los cuerpos macroscópicos (aves, autos, plantas, órganos internos, etc.). En la vida cotidiana podemos observar comportamientos que en tiempos antiguos fueron notados, descritos y analizados para realizar predicciones tanto por físicos, filósofos y matemáticos. Estos conocimientos fueron transmitidos, posteriormente, por profesores en escuelas, colegios y universidades, y muchos de ellos los utilizamos a diario o por lo menos si nos hablan de ellos sabemos los principios que los rigen. Además, a través de la percepción por medio de nuestros sentidos y los aparatos de medición, se han forjado ideas preconcebidas que nos dictan como deberían comportarse los elementos macroscópicos. Pero en el mundo atómico nada de esto es útil y puede parecer descabellado, ya que los resultados de la interacción de los sistemas atómicos y sus elementos no encajan con las leyes físicas clásicas propuestas.

Los físicos y filósofos pensaron por muchos años que el principio de causalidad tenía que ser parte esencial de toda ciencia, pues se tiene la expectativa de que siempre que existan las mismas condiciones tienen que generarse los mismos resultados o fenómenos. Pero a escala atómica y subatómica ni éste ni muchos principios como el determinismo, por ejemplo, tienen validez, pues pueden suceder diferentes efectos de una misma causa, cada una con su probabilidad de ocurrir, dado que a nivel atómico solo se pueden hacer predicciones o hablar de probabilidades. La localidad, objetividad y completez también están totalmente en duda a este nivel (Morrones, 2005).

Para entender los sistemas a escala atómica tenemos que aislar nuestras concepciones usuales, las realidades que generan nuestros sentidos y el sentido común pues tienen su sustento en observaciones y postulados que fueron llevados a una escala muy diferente como la que es observable a nivel humano, la macroscópica. Por lo mismo, el conocido físico Richard Feynman (1985) dijo: "*pienso que es seguro decir que nadie entiende la mecánica cuántica. Deje de repetirse, si puede evitarlo, la pregunta ¿pero cómo puede ser así?, ya que terminaría en un callejón sin salida del que nadie ha escapado aun. Nadie sabe cómo es que puede ser así.*".

El mundo microscópico es un extraño mundo. Requiere formular nuevas leyes que nos sirvan para explicarlo de manera correcta, aunque algunos físicos que están de parte de la interpretación Neo-Realista (también llamada variable oculta) se niegan a aceptar la idea de que la realidad pueda ser tan ambigua, desconcertante o improbable. Aducen que una vez descubiertos los valores de esta teoría que falta, se encontrará la familiaridad con las teorías clásicas que hacen uso de la realidad del sentido común.

La medición en Mecánica Cuántica.

Uno de los aspectos importantes de la teoría cuántica ha sido aceptar que la probabilidad es una característica elemental del mundo atómico. Los elementos subatómicos no se encuentran con seguridad en lugares definidos, sino como propuso Heisenberg, estos solamente muestran una tendencia a existir.

Además los acontecimientos a nivel atómico no suceden con exactitud en momentos y maneras definidas, sino que muestran una tendencia a ocurrir. Estas tendencias o probabilidades de las cuales hablamos no se refieren a probabilidades de los sucesos, sino a probabilidades de interconexiones. Esto porque un objeto atómico observado forma parte de un sistema intermedio y este no existe ni tiene significado como una entidad aislada, sino como una conexión entre procesos de medición y preparación. Las propiedades no pueden ser separadas de estos procesos ya que si estos sufrieran modificaciones igualmente ocurriría con las propiedades.

En la física atómica, la observación plantea un gran problema, que para definir un sistema observado este debe estar aislado; sin embargo para ello hay que estar necesariamente interactuando con el sistema (Walsh y Vaughan, 1982). Esta complejidad de aislar un elemento microscópico de un sistema para su observación sin evitar interactuar con el mismo y modificarlo, demuestra que no es posible descomponer el mundo en unidades mínimas con existencia independiente. Conforme estudiamos la composición de la materia nos damos cuenta de que está formada de partículas, pero no a manera de bloques de construcción, sino intrínsecamente relacionadas unas con las otras en un sistema. Esto se puede recalcar con lo mencionado por Bohr (1934): "*las partículas materiales aisladas son abstracciones, ya que sus propiedades sólo son definibles y observables mediante su interacción con otros sistemas*".

En el mundo atómico y subatómico el indeterminismo es una característica distintiva que imposibilita determinar las cantidades físicas de los elementos con la precisión requerida, así como la posición y la velocidad.

Contrario al mundo atómico, los sistemas macroscópicos pueden ser observados sin ocasionar alteraciones en el sistema. Por ejemplo, para medir la localización de poste, interaccionamos con él arrojándole luz, y el reflejo nos dirá donde está localizado; o una simple medición de un objeto con una cinta métrica.

Toda medición requiere interacción entre el equipo de medición y el sistema a medir. En el mundo macroscópico no ocurre ninguna perturbación sobre el objeto medido, si se toma como base los ejemplos anteriores; pero muy distinto ocurriría si intentáramos medir la posición del protón o electrón. Si a este último le aplicáramos luz para su medición, al comportarse como partícula (basado en la teoría dualidad "onda partícula") los fotones chocarían con los electrones perturbando el estado del sistema al aplicarle cierta cantidad de movimiento (Morrones, 2005).

Lo objetivo tampoco es ya característico en el mundo atómico como lo es a escala macroscópica pues no es posible observar un sistema sin ocasionarle modificaciones o alteraciones. Esto nos obliga a ver el universo como una telaraña de relaciones entre las distintas partes de un todo unificado y no como una colección de elementos físicos. Adicionalmente, para que una teoría sea "realista local" esta debe ser objetiva y local, y como vimos estos no están en la M.C. John Bell en 1964 aplicó un diseño experimental introducido a través de

unas desigualdades que llevan su nombre (desigualdades de Bell), para demostrar que la M.C. no es una teoría realista local (Greene, 1999).
Aun cuando la M.C. viola principios como localidad, objetividad o causalidad estos a escala macroscópica siguen teniendo validez.

Hechos experimentales.

La dualidad Onda-Partícula.

Por lo tanto, el concepto de partícula siempre ha sido descrito como una cantidad de materia en un espacio muy pequeño en relación al sistema que lo rodea como por ejemplo una gota de agua desprendida de una catarata si lo vemos a escalas mayores o incluso, los planetas del sistema solar dentro de una galaxia. Por otro lado, está la onda, la cual se extiende por una región del espacio sin una posición definida y tiene una descripción matemática abstracta que satisface una ecuación de onda (Morrones, 2005).

En el mundo cuántico estas diferencias conceptuales desaparecen ya que los átomos y sus elementos pueden tomar ambos comportamientos, como fue demostrado experimentalmente por Thomas Young en 1801.

Entre los principales misterios de la mecánica cuántica está la dualidad onda-partícula, ejemplificada por medio del famoso experimento de doble rendija, el cuál consiste en lo siguiente: se tiene una tarjeta con una rendija y se envía luz; una vez que esta es reflejada en esa tarjeta con una rendija, la luz pasa a través de ella y se refleja una banda de un tamaño proporcional a la abertura por donde pasa la luz, asumiendo el comportamiento de la luz como partículas y no como ondas.

Figura # 1
Reflejo de un as de luz

Fuente: Tomadas de http://www.youtube.com/watch?v=DfPeprQ7oGc.

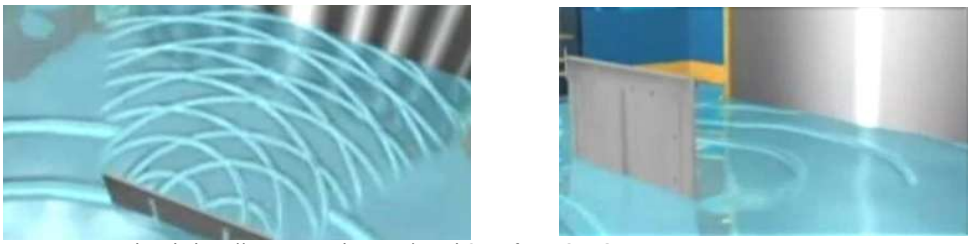
Si a esa tarjeta le hacemos otra rendija cerca de la existente, esperaríamos que se reflejara otra banda de igual tamaño proporcional junto a la que estaba ya hecha.

Figura # 2
Reflejo de dos ases de luz

Fuente: Tomadas de http://www.youtube.com/watch?v=DfPeprQ7oGc.

Pero lo interesante es que no pasa eso. Por ello los físicos en su momento, para tratar de explicar el fenómeno, lo atribuyeron al comportamiento ondulatorio de la luz, debido a que ocurría una interferencia que creaba bandas reflejadas de intensidades menores del centro hacia los lados como se ve en la ilustración. De esa forma también con una sola rendija se produciría el mismo reflejo o patrón de luz reflejado que tratando la luz como partículas.

Figura # 3
Reflejo de ases de luz con dos y una rendija con efecto ondulatorio.



Fuente: Tomadas de http://www.youtube.com/watch?v=DfPeprQ7oGc

Además decían que las partículas al chocar entre sí provocaban esas interferencias y por lo tanto ese patrón. Así que decidieron lanzar destellos de luz o segmentos de partículas para que estas no chocaran entre sí y no se formara ese patrón, pero se toparon con la sorpresa de que ocurría exactamente lo mismo. La explicación dada es que las partículas parten como una sola de su fuente, se convierte en una onda de probabilidad, atraviesa ambas rendijas e interfiere consigo misma para llegar a la pared como una sola partícula.

Para averiguar por cual de las rendijas pasaban las partículas repitieron el experimento de doble rendija y colocaron un observador o detector de partículas. Aquí es donde nace uno de los misterios de la física cuántica, pues con el observador al lado se comporta como partícula, formando las dos solamente, en cambio sin el observador se forma el patrón de interferencia con muchas bandas. Al intentar medir o de observar por cuál banda entra la luz o partículas, éstas deciden actuar de forma distinta como si supieran que se les está observando (Young, 1804).

Este patrón de comportamiento se presenta igualmente con los átomos y sus componentes, pero la luz sirvió como una iniciación para explicar el fenómeno dual onda-partícula de la materia.

El gato de Schrodinger.

Este es un ejercicio imaginario propuesto por el físico Erwin Schoringer en 1935. Propone un sistema compuesto por un gato, una caja cerrada, una botella con gas venenoso, un martillo que pende sobre la botella y un detector de partículas alfa.

El ejercicio comienza introduciendo el gato en la caja. Sobre ella al lado del detector de partículas, se coloca un átomo radioactivo con un 50% de posibilidades de emitir una partícula alfa en un periodo de tiempo determinado. Cuando este ha transcurrido puede o no haberse radiado la partícula alfa y activar el martillo que pendía sobre la botella que pudo haber quebrado o no la botella de veneno. Por lo tanto, el gato puede estar vivo o muerto, la única forma para saberlo es abriendo la caja. Aquí es donde el experimento arroja conclusiones interesantes ya que el gato está dado por una función compleja que provee como resultado la superposición de dos estados combinados (el gato vivo y el gato muerto). Esto implica que mientras la caja esté cerrada, el gato estaría muerto y vivo a la vez (Palazzesi, 2009).

Podríamos encontrarlo muerto o vivo solo si abrimos la caja, pero esto interactuaría con el sistema y lo modificaría quebrando la superposición de estados, y por tanto, definiéndose por uno de los dos estados. En la vida real un gato puede estar vivo o muerto pero no ambos, en cambio, en mecánica cuántica si puede tener los dos estados mientras no exista un observador, que puede ser cualquier dispositivo electrónico, sensor o humano. Es similar al experimento de doble rendija donde existe una superposición de estados debido a la naturaleza ondulatoria de la materia.

La Paradoja EPR.

La paradoja de Einstein-Podolsky-Rosen, denominada «Paradoja EPR», consiste en un experimento mental propuesto por Albert Einstein, Boris Podolsky y Nathan Rosen en 1935 (Wikipedia, 2009).

Esta paradoja va contra los postulados de Newton y su ortodoxa doctrina de las leyes de la física clásica. Critica los conceptos de no-localidad y de medición que han sido abordados secciones atrás.

El experimento consiste en tener un par de partículas simétricas con un origen o evento en común, las cuales se mantendrán relacionadas a través del entrelazamiento cuántico por una función de onda. Si separamos estas dos partículas correlacionadas de un extremo al otro del universo, sus propiedades deberán tener valores opuestos. Por ejemplo, si realizamos la medición de la partícula A con un valor de + 1, por su correlación la partícula B tendrá un valor de -1, aunque no la midamos (García del Cid, 1994). Esto es un misterio que Einstein trató de explicar durante su vida al considerar que existían variables ocultas que explicaran la paradoja; pero el físico John S. Bell pudo demostrar la paradoja científicamente: "*Ninguna variable local oculta puede explicar las correlaciones que se dan en la paradoja EPR, lo que deja abierta la posibilidad, aun cuando las separen años luz, de que las partículas permanezcan conectadas por un nivel subcuántico no local que nadie conoce*". (Bell, 1990).

Al interactuar con el sistema para realizar la medición de cualquier partícula entrelazada cuánticamente, se estaría obteniendo el valor de una y automáticamente de la otra, que a su vez también estaría cancelando su función de onda y por tanto modificando su estado físico o propiedades de forma inmediata; en otras palabras, sucede como si una partícula le dijera a la otra que está siendo observada o medida para que cambien su estado conjuntamente, aunque se encuentren a millones de años luz. Aquí surgen contrariedades en relación con la teoría de la relatividad. Esta establece que la velocidad mayor de traslación es la de la luz y no instantánea como para que una partícula A y B reaccionen inmediatamente al cambio de estado por observación o medición.

Sintetizando la idea, aunque nada viaja mas rápido que la velocidad de la luz, en el mundo cuántico con dos partículas relacionadas por una función de onda o entrelazadas cuánticamente, si es posible. Todo parece indicar que "cierta energía" es la promotora de esta correlación simultánea de conocimiento entre partículas, pero en física no se conoce una energía que pueda moverse tan rápidamente. Einstein, en 1935, se encontró con este efecto misterioso derivado de la mecánica cuántica, y lo tildó de "fantasmal" o "*spooky effect*" puesto que ampararía fenómenos paranormales hasta entonces desdeñados por la ciencia, como la telepatía. Einstein concluyó que debía haber algo radicalmente erróneo en la mecánica cuántica para permitir llegar a semejantes conclusiones. A raíz de esto, Einstein en una carta enviada al Dr. Jan Ehrenwald, el 8 julio de 1946 le dijo ¨ No tenemos derecho, desde un punto de vista físico, a negar a priori la posibilidad de la existencia de la telepatía¨ (García del Cid, 1994).

La Informática Cuántica.

La informática cuántica es la próxima revolución de las ciencias de la computación clásica, un paradigma distinto al que se ha desarrollado a través de la historia en las cinco generaciones de computadoras que nos enseñaron en las escuelas de informática.

Encontramos actualmente buscadores en internet que arrojan resultados en cuestión de segundos, supercomputadores como el del pentágono o la NASA, potentes *mainframes* como los de las líneas aéreas, poderosos computadores dedicados al diseño gráfico como los de DreamWorks Studios, etc. Éstos están compuestos por "hardware prohibitivo" para cualquier persona, al igual que software especializado que utiliza tecnologías *GRID* o *Cluster* para compartir recursos y ejecutar millones de cálculos y operaciones complejas en el menor tiempo posible y tratando de aprovechar al máximo los recursos disponibles.
Lo anterior ya está empezando a llegar a su límite máximo de capacidad lo que ha llevado a pensar en formas alternativas de innovar las arquitecturas de hardware y software para obtener mejor rendimiento y hacer valer la Ley de Moore que se ha venido cumpliendo desde que se propuso.

Una de estas formas de innovación es la miniaturización o nanotecnología, la cual ha sido pieza clave en la evolución de las generaciones de los microprocesadores. Estos han pasado a escalas microscópicas como los que

se encuentran actualmente en el mercado de 45 nm, producidos por empresas como Intel o AMD. Este proceso de reducción ha mejorado rendimiento de procesamiento, reducción de latencia en componentes como memorias volátiles, menor calentamiento, la disminución de uso energético, de espacio físico, entre otros.

El factor innovador de la miniaturización está llegando a su punto máximo, pues está tocando un límite donde difícilmente es posible para la maquinaria y procesos de producción actuales reducir a menor escala. Por esta razón, se tiene que cambiar el esquema tradicional seguido hasta el momento por la computación clásica e incorporar nuevas formas de procesamiento, ayudados ya no por componentes físicos muy diminutos, sino por estructuras microscópicas a nivel atómico y molecular, las cuales no se rigen por las leyes newtonianas o de física clásica, sino por las leyes de la mecánica cuántica y los factores propios del comportamiento en su entorno como los sintetizados en apartados anteriores.

A partir de este cambio es donde se empiezan a plantear teorías, procedimientos y nuevas propuestas para el uso de la informática cuántica y su incorporación en procesos actuales como: aumento de la capacidad de procesamiento de instrucciones, incremento en las capacidades de almacenamiento, comunicaciones cuánticas y mejora en el rendimiento del software mediante el uso de algoritmos cuánticos.

En cuanto al procesamiento se plantea un cambio significativo respecto a la forma clásica de procesar la información, pues se hacía uso del sistema de numeración binario tomando los datos forma de bits donde 0 o 1 eran la unidad mínima, que es lo mismo en álgebra booleana que falso o verdadero. Al utilizar la forma cuántica, existiría una superposición o combinación lineal de estados, o sea que un 0 o 1 podrían corresponder al *spin* de un átomo o algún componente del mismo como el electrón, pero también pueden encontrarse en una superposición de ambos estados (llamado estado qubital puro), 0 y 1 al mismo tiempo. Como puede tomar ambos estados a la vez, surge un paralelismo cuántico con combinaciones como 00, 01, 10 y 11, lo cual dobla la representación de los bits. A esta unidad mínima que constituye la informática cuántica se le llama qubit.

Por analogía, se puede entonces concluir que el qubit ofrece mayor cantidad de opciones que el bit, lo que aumenta la capacidad de los componentes computacionales. Si se implementara en un software de diseño gráfico el uso de algoritmos cuánticos, el usuario final podría ver incrementado el rendimiento y las mejoras en imágenes al existir mayor capacidad de combinación de colores, lo que supone una nueva forma de resolver tareas y ciertos problemas. Igualmente, si fuera en un sistema de reservaciones en línea o cálculo de operaciones matemáticas complejas se podrían obtener más transacciones u operaciones por segundo.

Sin embargo, actualmente científicos e ingenieros enfrentan problemas para solventar la ambigüedad en el tratamiento de los datos que se le imponen al sistema, teniendo en cuenta que este es más similar a la forma en cómo piensa

la mente humana que a la de un computador binario. Según una investigación de la Universidad de Cornell, se identificó una mayor similitud de la mente humana con los procesos cuánticos que con la informática tradicional, se evidencia a está moviéndose en un continuo, desde la superposición de opciones ante la toma de una decisión. Se tomó como muestra 42 estudiantes que tenían que escoger una imagen en la pantalla de una PC según la palabra que ellos escuchaban. Cuando escucharon un término relacionado completamente con una de las figuras que se comparaban entre sí, se trazó un camino directo del mouse hasta el objeto correcto, pero cuando la palabra tenía una similitud con ambas opciones, la elección resultó ser lenta y con una dirección curva, lo que significa que la mente así como la informática cuántica no opta por 0 ó 1, sino que desarrolla estadios de oposición hasta llegar al final (Yanover, 2007).

Teleportación Cuántica.

Teletransportación cuántica es la transferencia de pequeñas unidades de información de la computadora, llamadas bits cuánticos o qubits, de un lugar a otro. La tecnología se conoce como un tipo de "teletransportación" ya que la información "teletransportada" se comporta más como un objeto de información normal que como materia o energía (Roach, 2003).

Los científicos tratan la información cuántica como si fuera un objeto. Como la información no puede ser transmitida sin ser destruida, también se diferencia la teleportación cuántica de enviar por fax un documento, ya que hace imprecisa una réplica del original en otro lugar y dejar intacto el original; la teleportación no es una cuestión de mover la materia, sino de transporte de información. Los físicos han sido capaces de intercambiar información exitosamente entre las partículas de luz (fotones) o entre los átomos, mientras que las partículas entrelazadas están lejos una de la otra.

Científicos del *Joint Quantum Institute (JQI)* llevaron a cabo un experimento, el primero en que la información recorrió una gran distancia: 1 m o un poco más de tres pies, entre dos átomos aislados. Es también la primera vez que los poderes de un fotón - que es especial para viajar a grandes distancias - y un átomo - que es apreciado por su capacidad para retener la información - han sido explotados conjuntamente (Dowling, 2009).

Un pulso de láser ultra-rápido provoca que los átomos emitan fotones simultáneamente. Si los fotones interactúan de manera correcta, sus átomos entran en un estado cuántico conocido como entrelazamiento (*entanglement*). En este estado, en la que el átomo B adopta las propiedades de un átomo A a pesar de que están en cámaras separadas por un metro de distancia. Cuando se mide A, la información que había sido previamente codificada desaparece, de conformidad con las normas peculiares del mundo cuántico. Pero no todo está perdido: B, al enredarse con A, ahora contiene la información que una vez fue llevada por A. Esta información, en un sentido muy real, se ha *teletransportado*.

El entrelazamiento cuántico, por el cual dos o más objetos están unidos por una conexión invisible, tiene algunos efectos como el famoso "*spooky effect"*

desarrollado por Einstein. Investigadores cuánticos como Anton Zeilinger, han dicho que el entrelazamiento puede ser pensado como un par de dados que siempre caen en el mismo número (Zeilinger, 2000).

La teleportación cuántica ha sido demostrada a través de distancias macroscópicas: cientos de metros en al menos un caso por fotones (Roach, 2003), partículas fundamentales de la radiación electromagnética, pero los iones son mejores candidatos para la memoria cuántica ya que pueden almacenar información durante periodos relativamente largos de tiempo.
Esta transmisión cuántica de información podría constituir la columna vertebral de comunicación a larga distancia (a velocidades inimaginables), pero ese tipo de red apenas se visualiza en un lejano horizonte.

Software Cuántico.

Feynman (1982) sugiere que la construcción de ordenadores basados en los principios de la mecánica cuántica podría permitir que los sistemas cuánticos, de interés para los físicos, sean emulados de manera eficiente, mientras que esto parece ser muy difícil con los ordenadores clásicos. Deutsch (1985) investigó la potencia de cálculo posible de los equipos de cómputo, y formuló una versión cuántica de la máquina de Turing. Esta establecía la posibilidad de construir un ordenador universal que podría programarse para simular cualquier sistema físico finito operado con recursos limitados. Shor (1994), de los laboratorios AT&T de la compañía Bell, demostró que dos importantes problemas prácticos como factorizar números enteros en factores primos y el problema de "logaritmo discreto" podrían resolverse de manera eficiente por los ordenadores cuánticos. Grover (1996) demostró mediante el desarrollo de un programa cuántico que la búsqueda en bases de datos también podría ser más eficiente mediante el uso de los ordenadores cuánticos, específicamente buscar información en una base de datos no “indexada” en tiempo proporcional a la raíz cuadrada del número de datos. Desde entonces, se ha desarrollado literatura importante en relación con los algoritmos cuánticos y teoría de la complejidad cuántica.

Otro tema importante en la invención de software cuántico ha sido el desarrollo de técnicas de criptografía cuántica, al cual se le dedicará en la próxima sección un apartado para una explicación más minuciosa. Existe una interesante interacción entre la computación cuántica y criptografía cuántica: siendo el algoritmo de Shor para la factorización de enteros, tiene el potencial de socavar muchos criptosistemas actuales: los sistemas de criptografía cuántica pueden ser protegidos entonces contra cualquier forma de ataque, incluidos los ataques que hagan uso de la computación cuántica.

Pero las novedades a nivel de programación no solo están inmersas en la criptografía, sino en la lógica de programación por parte de los desarrolladores. En la computación clásica, las instrucciones deben indicar secuencialmente todas las posibles alternativas a analizar, y dependiendo de las condiciones o datos presentes, se alcanza la solución por un determinado camino. Pero los algoritmos cuánticos tienen que pensar en expresiones de superposición, es decir, se debe escribir el código de un software tomando en cuenta todas las alternativas posibles de solución al mismo tiempo.

A pesar de la observación de Deutsch (1985) de que "los ordenadores cuánticos plantean problemas interesantes para el diseño de los lenguajes de programación", los informáticos han sido lentos para responder a este desafío.

El hecho de que las implementaciones de física cuántica en los ordenadores son todavía muy limitadas, trabajando sólo unos pocos qubits y que todavía no han escapado de los laboratorios de física, expone el ámbito de los lenguajes de programación cuántica a la crítica, ya que no es útil estudiar lenguajes de programación para hardware inexistente. Algunos científicos aducen que esta crítica es infundada, por varias razones.

En primer lugar, pasa por alto el espectacular progreso que se ha hecho en la aplicación práctica de los sistemas de criptografía cuántica. Los componentes de estos sistemas ya están disponibles comercialmente, y parece muy probable que la criptografía cuántica será una importante tecnología mucho antes de que los ordenadores cuánticos de tamaño útil sean construidos.

En segundo lugar, el uso generalizado de los lenguajes de programación que no tienen una firme base semántica ha causado enormes problemas para la ingeniería de software. Tecnologías informáticas prácticas han ido delante de los estudios teóricos, y sólo recientemente los últimos desarrollos del diseño de lenguajes de programación (por ejemplo, Java 1.5) han tenido el beneficio de una base teórica que fue bien entendida por adelantado. Desde este punto de vista, el diseño de lenguajes de programación cuántica antes de que exista hardware es, en algunos aspectos, una situación ideal.

En tercer lugar, y tal vez de forma inesperada, la aplicación de la semántica, lógica y en especial las técnicas de la teoría están proporcionando una nueva perspectiva fascinante sobre la teoría cuántica. Informáticos están generando nuevos conocimientos sobre los fundamentos de la mecánica cuántica que serán de gran valor, incluso si las computadoras cuánticas nunca se construyen.

Hay mucho espacio para la investigación adicional en todas las áreas de aplicación de lógica cuántica en el software. En el diseño del lenguaje, el uso de estructuras de datos complejas cuánticas no ha sido totalmente explorado, ni el desarrollo de las estructuras de control de alto nivel cuántico. Ha habido relativamente menos énfasis en la semántica formal de los lenguajes imperativos que para los lenguajes funcionales y sería útil para restablecer el equilibrio. Una semántica denotativa de mayor cálculo para funciones u operaciones cuánticas todavía no está resuelta. El área de la compilación de lenguajes de programación cuántica ha recibido relativamente poca atención.
Como en los lenguajes viene a ser posible un incremento en complejidad y las implementaciones prácticas, las sofisticadas técnicas de la teoría clásica del compilador pueden ser muy relevantes para la aplicación cuántica.

La implementación física de los ordenadores cuánticos es un área de investigación activa, y no está claro aún cuál tecnología física será la más exitosa. Esto tiene implicaciones para el lenguaje de programación y el diseño

del compilador: cualquier implementación de tecnología puede tener una serie preferida de operadores y medidas que son más fáciles de implementar.
Puede que sea necesario desarrollar una gama de técnicas de compilación dirigidas a diferentes arquitecturas físicas, o una gama de características de lenguaje de programación diseñado para explotar las operaciones preferidas de los diferentes esquemas de implementación (Simon, 2005).

Criptografía Cuántica.

Según la enciclopedia en línea Wikipedia (2009), la criptografía se define como una disciplina que trata de la transmisión y almacenamiento de datos de manera que no puedan ser comprendidos ni modificados por terceros. Por su parte, la criptografía cuántica se entiende igual, pero se le suman principios de mecánica cuántica para garantizar la absoluta confidencialidad de la información transmitida.

En la actualidad el medio más rápido de trasmisión de información es la fibra óptica el cual utiliza pulsos de luz para representar los datos que quiere transmitir. Estos pulsos de luz están compuestos por fotones los cuales son unidades o elementos utilizados individualmente para la criptografía cuántica al utilizar sus dos estados de polarización para superponer o entrelazar el estado del qubit. Esta rama de la física cuántica está sustentada en el principio de incertidumbre de Heisenberg, según el cual, como ya se mencionó, no se puede conocer la posición ni la velocidad exacta de un elemento atómico en determinado instante, además de que cualquier proceso de medición de éstas variables modifica el sistema y el estado de la partícula. Dado lo anterior, sólo con el uso de filtros para detectar la polarización, que es utilizada como soporte físico de un estado cuántico, puede ser implementada en la comunicación una criptografía cuántica. Sobre esta polarización se puede mencionar que hace uso de dos filtros, uno para diferenciar entre fotones con polarización horizontal o vertical y otro para diferenciar entre fotones con polarización inclinada hacia la derecha o izquierda (Wikipedia, 2009).

La seguridad de los sistemas cuánticos se basa en que el remitente y el destinatario comparten una llave aleatoria prácticamente indescifrable. Si alguien intentara husmear el intercambio de llaves, el solo acto de ver los fotones hace que estos cambien, siguiendo las leyes de mecánica cuántica. Esto sería perceptible por los usuarios al ver un incremento mayor al 50% en la tasa de errores de transmisión, por lo que sería imposible que alguien pudiera descifrar la información transmitida sin dejar rastros y alterar los estados de los fotones.

Lo anterior está sustentado en tres principios (Baig, 2008):

1. Teorema de "no clonación" nos afirma que no puede ser copiado un estado cuántico. Al menos en la teoría aún no existe una fotocopiadora cuántica.
2. El intento de obtener la información cuántica de un qubit puede implicar una alteración del mismo y del sistema, o destrucción de la información que porta. Dado lo anterior, es imposible obtener información sin modificar los datos que están siendo transmitidos.

3. La medición cuántica es irreversible. Después de realizar una medición no se puede regresar el sistema manoseado por terceros al estado que tenía antes de la medición, o sea alguien que quiera espiar siempre dejará rastro y no lo podrá camuflar.

Esta tecnología se ha implantado en organizaciones gubernamentales y empresas privadas que pueden pagar los altos costos que conllevan. Además, en la mayoría se encuentra la conexión directa o punto a punto a través de fibra óptica. Empresas como Siemens han llevado a cabo conexiones de redes cuánticas en cinco de sus sucursales con distancias máximas de hasta 82 kilómetros. Esta empresa junto con 40 socios de 12 países forman parte del proyecto SECOQC (*Development of a Global Network for Secure Communication based on Quantum Cryptography*) quienes realizan el mismo proyecto en sus empresas dentro de la Unión Europea (SECOQC, 2008).

Computadora Cuántica.

Búsquedas en bases de datos de Petabytes, ejecución de algoritmos cuánticos, creación de encriptaciones indescifrables y mucho más son aplicaciones que están lejos de ser ejecutadas en las computadoras de hoy, pero sí podrían ser ejecutadas en segundos por computadoras cuánticas, que teóricamente están basadas bajo la mecánica cuántica, entendida como una física teórica dedicada a la materia y energía a nivel atómico.

Aunque los ordenadores se han vuelto más compactos y mucho más rápidos en el desempeño de sus tareas, su tarea sigue siendo la misma: para manipular e interpretar una codificación de bits en un resultado de cálculo de utilidad. Un bit es una unidad fundamental de la información, clásicamente representado como un 0 o 1 en un ordenador digital. Cada bit clásico se recrea físicamente a través de un sistema físico macroscópico como la magnetización en un disco duro o la carga de un condensador. Un documento, por ejemplo, compuesto de n-caracteres almacenados en el disco duro de un ordenador típico es descrito por una serie de ceros y unos.

En un ordenador cuántico las normas han cambiado. No solo puede existir un bit cuántico, usualmente llamado qubit, en los estados clásicos de 0 y 1, sino también puede estar en una posición coherente de ambos. Cuando un qubit se encuentra en este estado puede ser considerado como existente en dos universos, como un 0 en un universo y como un 1 en el otro.

Esto puede parecer contradictorio debido a que los fenómenos cotidianos son gobernados y explicados por la física clásica y no la mecánica cuántica, la cual toma el relevo en el nivel atómico. Una operación en qubit actúa efectivamente sobre ambos valores al mismo tiempo. El punto importante es que se realiza la operación única en el qubit, generando una operación en dos valores diferentes. Asimismo, un sistema de dos qubits podría realizar la operación sobre cuatro valores, y un sistema de tres qubits en ocho. Por lo tanto, al incrementar el número de qubits aumenta exponencialmente el "paralelismo cuántico" que se puede obtener con el sistema. Con el tipo correcto de algoritmo es posible utilizar este paralelismo para resolver determinados problemas en una fracción del tiempo requerido por una computadora clásica.

Para explicar más detalladamente lo anterior, una computadora tradicional trabaja sobre bits que representan estados de 0 o 1, o sea lenguaje binario. En el procesamiento de datos cuánticos se propone la sustitución de estos bits por bits cuánticos o qubits. Estos podrían estar ya sea en estado 0 o 1 pero también por privilegio del mundo cuántico, en una superposición de ambos, 0 y 1 al mismo tiempo y en diferentes proporciones (por ejemplo, el 25% de 0 y 75% de 1: esto significa que cuando el valor del qubit es medido, hay 25% de posibilidades de encontrar 0 y 75% de encontrar 1) (Parodi y Wacrenier, 2009). La unidad de medida de las computadoras cuánticas (qubit) utiliza una lógica mucho más compleja que involucra múltiples estados de entrelazamiento, lo que permite un procesamiento eficiente de nuevos sistemas de información. El físico austriaco Erwin Schrödinger acuñó el término entrelazamiento o "*entanglement*" para describir la peculiar conexión entre los sistemas cuánticos, por ejemplo, cuando las partículas muestran una distribución de los estados de intercambio de información.

El entrelazamiento cuántico ("*Quantum Entanglement*") corresponde a propiedades no locales de partículas entrelazadas formando una red reticular híbrida, que permite calcular en paralelo varios estados de información simultáneamente, a diferencia de bits clásicos que sólo tienen un valor en el tiempo. Por lo tanto, dicho entrelazamiento es el ingrediente necesario de la Computación Cuántica y puede ser contemplado como un paralelismo de superposición de estados, de un conjunto de información cuántica de estado simultanea. La transferencia de este estado de entrelazamiento cuántico a un lugar arbitrario distante es conocido como "*entrelazamiento de tele-transporte asistido*", el cual no intercambia energía o materia, sino solo información pura y con la particularidad de que la transferencia de la información del estado ocurre de forma simultánea (Reck y Kwiat, 2009).

El truco en la computación cuántica es aprovechar el entrelazamiento de las diferentes partículas, lo que Einstein llamó la "fantasmal acción a distancia o *spooky effect*", que permite que una partícula afecte a otra donde quiera que sea.

A principios de 2007 la empresa canadiense D-Wave Systems afirmó que logró demostrar la resolución de procesos complejos y altas capacidades de procesamiento en un equipo cuántico llamado Orion. Según la compañía, la demostración efectuada es un gran paso adelante para la solución de los problemas comerciales y científicos que se consideraban sin solución hasta ahora. Orion hace uso de principios cuánticos por medio de anillos de corriente que fluyen a través de los superconductores. La corriente puede fluir hacia la derecha, la izquierda o significativamente en ambas direcciones a la vez, lo que le permite tener dos valores al mismo tiempo debido a la extraña mecánica cuántica.

Sin embargo, muchos sectores de la informática han manifestado sus dudas con respecto al computador cuántico, especialmente porque D-Wave Systems ha publicado muy poca información acerca de su máquina y la demostración en sí no fue muy impresionante. Se dice que la empresa puso de manifiesto

problemas que pudieron haberse resuelto con ordenadores clásicos en un tiempo razonable (Amit, 2008).

Conclusiones.

Las computadoras cuánticas utilizan qubits o bits cuánticos en lugar de bits clásicos para representar y procesar la información. Esto da lugar a nuevas maneras de resolver problemas o diseñar programas y usa para ello nuevas puertas lógicas y algoritmos cuánticos como los mencionados en este artículo. Toda esta nueva lógica se rige bajo los principios de las leyes de mecánica cuántica y su comportamiento antagónico con respecto a nuestra clásica manera de explicar el comportamiento del mundo macroscópico que es percibido por nuestros sentidos.

En teoría, los ordenadores y algoritmos cuánticos proveen posibilidades de realizar cálculos con una abismal eficiencia con respecto a los ordenadores clásicos, debido a la superposición de estados en qubits y las posibilidades de factorización.

Algunas aplicaciones han empezado a ser comercializadas con el emblema de tecnología cuántica como el caso de la criptografía, la cuál propone un innovador enfoque, como lo es “seguridad total” en las comunicaciones a causa de a la posibilidad de realizar operaciones de factorización a velocidades imposibles para una computadora de hoy.

Nuevamente nos encontramos con otra revolución interdisciplinaria que viene a modificar, particularmente en informática, las técnicas de las tecnologías de información utilizadas para procesar datos y generar información. La construcción de ordenadores cuánticos podría permitirnos estudiar nuevas formas de tratar la información y reafirmar los comportamientos cuánticos que han sido ligeramente observados por algunos científicos en laboratorios y explicados mediante ejercicios mentales como el Experimento de Doble Rendija o el Gato de Schrodinger.

Si la situación actual es similar a la que existía hace casi medio siglo cuando se construyó el primer computador, y además la famosa Ley de Moore sigue el mismo comportamiento, cada 18 meses se duplica el número de transistores en un circuito integrado, entonces la única forma de explicar como incrementar esta capacidad sería llevando los modelos de arquitecturas de procesamiento a niveles atómicos debido a la miniaturización, que está llegando a su máxima capacidad.

El futuro de hardware de ordenador cuántico es probable que sea muy diferente de lo que hoy conocemos; sin embargo, la investigación actual ha contribuido a proporcionar una visión sobre qué obstáculos traerá el porvenir para estos dispositivos.

Teniendo en cuenta las dificultades de manipulación de los átomos, el número máximo de los qubits que podrían ser llevados a los prototipos más recientes de ordenador cuántico no exceden los 7 qubits. La comercialización de la primera calculadora cuántica está prevista para el 2020.Esta utilizará una docena de qubits. Inicialmente, el objetivo será el asociar los procesadores cuánticos con los procesadores tradicionales, a fin de llevar a cabo las

operaciones más costosas en menos tiempo que los primeros. El equipo tradicional enviaría entonces las operaciones cuánticas a la maquina de estados cuánticos mediante el uso de continuaciones de las órdenes o algoritmos en lenguaje QCL. De esta forma, esta calculadora entregaría los resultados que serian analizados por el procesador tradicional. Todavía estamos lejos de un equipo cuántico completo (Parodi y Wacrenier, 2009).

Algún día gracias a las características de no locación y el entrelazamiento de la mecánica cuántica, la información podría compartirse sin recorrer distancias y las computadoras incrementarían en millones de instrucciones las capacidades de ejecución que los ordenadores clásicos durarían años resolviendo.

Referencias Bibliográficas.

Amit, The Tech FAQ (2008). Everything You Wanted to Know About Quantic Computers. Recuperado el 03 de noviembre del 2009, de http://www.thetechfaq.com/2008/03/06/everything-you-wanted-to-know-about-quantic-computers/

Ball, David W. (2001). The Basics of Spectroscopy. Bellingham, WA, USA: SPIE- The International Society for Optical Engineering.

Bell, John S (1990), Lo decible y lo indecible en la mecánica cuántica, Madrid, España. Alianza Universidad.

BOHR, Niels (1934). Atomic Theory and the Description of Nature, Cambridge: Cambridge University Press.

Deutsch, D. (1985) Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London A 400:97–117.

Dowling, Danielle (2009) Teleportation Is Real – But Don't Try It at Home. Recuperado el 05 de noviembre del 2009, de http://www.time.com/time/health/article/0,8599,1874760,00.html

Einstein, Albert (1948). «Quanten-Mechanik und Wirklichkeit». Dialectica 2: 320 - 324.

F. Parodi & V. Wacrenier (2009). Quantic Computing - A travel into qubits…. Recuperado el 03 de noviembre del 2009, de http://kastor1337.info/EPITA/Quantum%20Computing.pdf

Feynman, Richard (1982). Simulating physics with computers. International Journal of Theoretical Physics 21(6–7):467–488.

Feynman, Richard (1985). QED: The Strange Theory of Light and Matter. Princeton University Press.

García del Cid, Lamberto (1994). La paradoja Einstein-Podolsky-Rosen y el teorema de Bell. Recuperado el 24 de octubre del 2009, de http://www.redcientifica.com/doc/doc200208140300.html

Greene, Brian (1999). The Elegant Universe. New York City, USA: Vintage.

Grover, L. (1996) A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on the Theory of Computation, pages 212–219. ACM Press. Also arXiv:quant-ph/9605043.

Kl-Khalili, J. Quantum (2003). A Guide for the Perplexed. New York, NY: Weidenfield & Nicolson.

M. Baig (2008). Criptografía Cuántica. Grupo de Física Teórica. Universidad Autónoma de Barcelona, España.

M. Reck and P G Kwiat (2009). Entangled Photons. Recuperado el 04 de noviembre del 2009, de http://physicsweb.org/objects/world/15/11/9/photons.pdf

Mackey, George W. (1963). "The mathematical foundations of quantum mechanics", New York, W. A. Benjamin.

Menas Kafatos, Robert Nadeau, (1999).The Conscious Universe: Parts and Wholes in Physical Reality (Paperback). Springer; 2nd edition.

Morrones, Rubén (2005). Los misterios del mundo cuántico. México, Facultad de Ciencias Fisico Matemáticas, UANL.

NASA (2009). LCROSS Viewer's Guide. Recuperado el 09 de octubre del 2009, de http://science.nasa.gov/headlines/y2009/05oct_lcrossvg.htm

Palazzesi, Ariel (2009). La paradoja del gato de Schrödinger. Recuperado el 23 de octubre del 2009, de http://www.neoteo.com/la-paradoja-del-gato-de-schrodinger.neo

R. Motwani and P. Raghavan, (1996). Randomized Algorithms. Cambridge: Cambridge University Press.

Roach, John (2003) Physicists Teleport Quantum Bits Over Long Distance. Recuperado el 31 de octubre del 2009, de http://news.nationalgeographic.com/news/2003/01/0129_030129_teleport.html

SECOQC (2008). World première in Vienna: Quantum Cryptography Secures Communication in a Commercial Network. Recuperado el 31 de octubre del 2009, de http://www.secoqc.net/downloads/pressrelease/SECOQC_PRESS%20RELEASE_english.pdf

Shor, P. W. (1994) Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, pages 124–134. IEEE Press.

Simon J. Gay (2005) Quantum Programming Languages. Glasgow G12 8QQ, UK, Department of Computing Science, University of Glasgow.

Walsh, R. & Vaughan, F. (1982). Más allá del Ego. Barcelona, Kairos.

Wikipedia (2009). Criptografía cuántica. Recuperado el 29 de octubre del 2009, de http://es.wikipedia.org/wiki/Criptografia_cuantica

Wikipedia (2009). Paradoja EPR. Recuperado el 24 de octubre del 2009, de http://es.wikipedia.org/wiki/Paradoja_EPR

Yanover, David Alejandro (2007). Pensar la Informática Cuántica. Revista Latinoamericana de Comunicación CHASQUI, número 099. Quito, Ecuador. Centro Internacional de Estudios Superiores de Comunicación para América Latina.

Young, Thomas (1804). Experimental Demonstration of the General Law of the Interference of Light, "Philosophical Transactions of the Royal Society of London", vol 94. London, UK.

YouTube (2009). Dr Quantum - Double Slit Experiment. Recuperado el 23 de octubre del 2009, de http://www.youtube.com/watch?v=DfPeprQ7oGc

Zeilinger, Anton (2000) “Quantum Teleportation”. NY, USA. Scientific American, August 2007 Issue.