COMPUTACIÓN CUÁNTICA

LEYDI ROCÍO CAMARGO QUINTERO
COD. 160002103

LAURA CONSTANZA OSORIO OVALLE
COD. 160002122

COMPUTACIÓN CUÁNTICA

INTRODUCCIÓN

Las profundas y fuertes investigaciones científicas encaminadas a descubrir y desarrollar nuevos métodos para mejorar y optimizar los procesos que hoy día conocemos, abren una nueva ventana donde descubrir las nociones, interpretaciones y avances se convierte en una tarea indispensable para el aprovechamiento y compresión del mundo tecnológico actual.

El paradigma de la computación cuántica es un tema vasto y emergente que nos introduce a múltiples campos en los que se fundamenta para su constante desarrollo, abarca desde la teoría de la información clásica hasta la física de partículas, pasando por la informática y la teoría matemática del tratamiento de la información.

La búsqueda constante de avanzar en la velocidad de procesamiento y en la capacidad de almacenamiento de los ordenadores, ha llevado a utilizar los conceptos y conocimientos más actuales en el campo de la física y matemática para implementarlos hasta el punto donde estos lo permitan y obtener una nueva forma de procesar la información utilizando los sistemas cuánticos, debido a sus características, pues cumplen con la necesidad de realizar las funciones de una maquina computacional tradicional en menor tiempo y con resultados más eficientes. Toda esta búsqueda va de la mano con el enfoque a la miniaturización que el mundo actual presenta y las limitaciones que muestra el Transistor al hacerse más pequeño, presentando al mundo la concepción de la Computación Cuántica sus ventajas y la proyección que brinda al progreso de la tecnología y el notable cambio que se está viviendo.

COMPUTACIÓN CUÁNTICA

Para hablar de computación cuántica, es necesario tener algunas nociones de conceptos relacionados con la teoría cuántica. La teoría cuántica "**es un conjunto de nuevas ideas que explican procesos incomprensibles para la física de los objetos" (Mario Toboso),** se basa netamente en probabilidades, determinando el estado y momento del acontecer de un suceso. Su aplicación recae en niveles atómico, subatómico y nuclear, con los aportes de este pilar se han dado explicaciones a fenómenos que la física clásica no podía argumentar. Utilizando la mecánica cuántica, como la rama de la física más actual, es posible explicar el comportamiento de la materia y de la energía, por medio del estudio de los átomos y las partículas elementales.

Las computadoras usadas hasta el día de hoy se basan en un sistema lineal, la unidad de información básica se conoce como el bit el cual se mide por impulsos voltajes eléctricos, que puede tomar dos estados 0 o 1. De este concepto se desprende toda la teoría informática, la base del almacenamiento de la información, algoritmos, lenguajes de programación y el hardware usado para implementar los modelos computacionales.

Cuando se plantea la computación cuántica, hay que remitirse a una nueva unidad básica de información: el Qubit, el cual tiene más complejidad que el bit.

QUBIT

El Qubit es la unidad elemental de la información cuántica, se encuentra niveles subatómicos, menores o iguales que la escala de nanos. Para entender los estados que puede tomar un Qubit hay que saber que las partículas subatómicas logran existir en múltiples estados de forma simultánea adoptando un estado de abierto, de cerrado o de ambos a la vez.

Los dos estados básicos de un qubit son $|0\rangle$ (ket cero) y $|1\rangle$ (ket uno), que corresponden al 0 y 1 del bit clásico. Pero además, el qubit puede encontrarse en un estado de superposición cuántica, combinación de esos dos estados ($\alpha |0\rangle + \beta |1\rangle$), lo cual marca la gran diferencia con respecto al bit.

"Un sistema cuántico se dice que tiene n qubits si tiene un espacio de Hilbert de 2 a la n dimensiones y dispone por tanto de 2 a la n estados cuánticos mutuamente ortogonales". **(Sergi Baila Martinez),** a pesar de la abstracción del término se puede hacer una comparación para entender las magnitudes de capacidad que se pueden alcanzar con esta unidad de información:

Un registro de tres bits, puede almacenar uno de los ocho valores posibles: 000, 001, 010, 011, 100, 101, 110, 111. En contraste un registro de tres Qubits puede almacenar en un estado determinado simultáneamente los ocho valores dados.

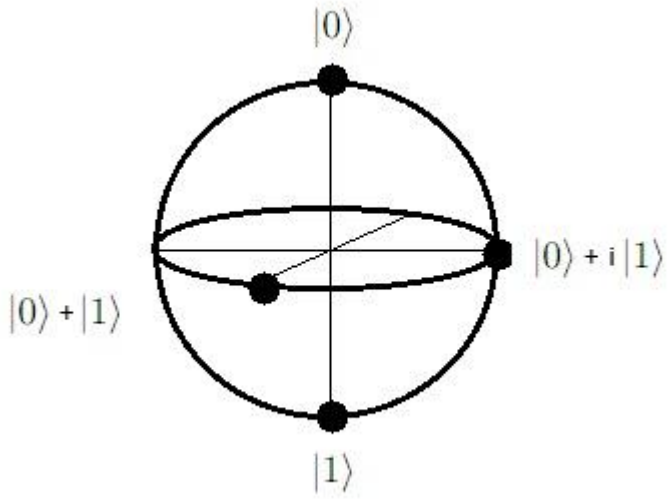

Figura 1. Representación de Qubit
Puede describirse como un vector de módulo unidad en un espacio vectorial complejo bidimensional.

MAQUINA DE TURING

Es un autómata o maquina matemática abstracta que se mueve sobre una secuencia lineal de datos. El modelo consiste en que cada instante la máquina lea un solo dato de la secuencia (generalmente un carácter) y realiza ciertas acciones en base a una tabla que tiene en cuenta su "estado" actual (interno) y el último dato leído. Entre las acciones está la posibilidad de escribir nuevos datos en la secuencia; recorrer la secuencia en ambos sentidos y cambiar de "estado" dentro de un conjunto finito de estados posibles.

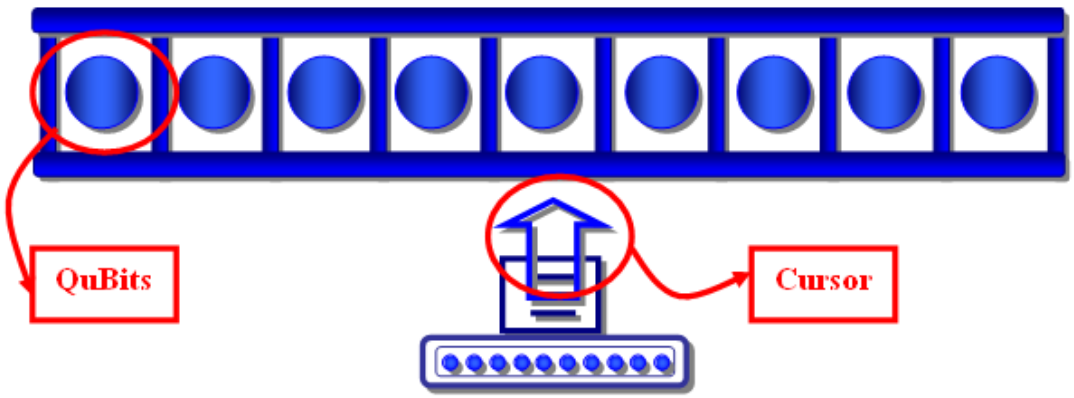

Figura 2. Máquina de Turíng cuantica

Un computador clásico se basa en el modelo de máquina de turing, al plantear una máquina de turing cuántica se hace posible la idea de una computadora cuántica. En 1985 Deutsch, presentó el diseño de la primera Máquina Cuántica. El modelo cuántico se diferencia por almacenar datos de Qubits en lugar de bits, de forma similar tiene los mismos componentes que el modelo clásico: un procesador finito y un cursor como se muestra en la figura 2.

PUERTAS CUÁNTICAS

Recrear nuevas compuertas lógicas para los Qubits abre un abanico de posibilidades para la generación de nuevos algoritmos, las puertas cuánticas son las operaciones básicas que se pueden hacer en Qubits, estas tienen una característica particular y es la reversibilidad.

DESARROLLO HISTÓRICO

Los científicos en el siglo XX exploraban métodos donde los recursos físicos (materia, fuerza y energía) eran los protagonistas de la escena científica. Sin embargo, un nuevo agente entra en el juego de los recursos, el cual se puede manipular y se rige bajo unas leyes físicas comprobadas, denominado como información. Inherente a este agente se encuentra la invención de la computadora capaz de procesar la información de una forma lógica y rápida en comparación a la mente humana. Pero que sucede con los procesos que necesitan mayores recursos y más velocidad de procesamiento que ofrecer una computadora tradicional, es en ese momento aparece el concepto de Computación Cuántica y la revolución que ha generado desde su concepción.

Para 1981 surgieron en la mente de **Paul Benioff** las ideas esenciales de la computación cuántica, Benioff trabajaba en el Argone National Laboratory en Illinois y teorizó un ordenador tradicional (máquina de Turing) operando con algunos principios de la mecánica cuántica. De igual manera, el físico Richard Feynman estableció en 1981 que teóricamente cualquier sistema físico podría ser simulado en una computadora cuántica. Una computadora cuántica supuestamente sería capaz de procesar varios fragmentos de datos al mismo tiempo alcanzado y exponía que dada su naturaleza algunos cálculos de gran complejidad se realizarían más rápidamente en un computador cuántico con procesamiento impresionante. En 1982 **Feynman** trabajó sobre la simulación de objetos mecánico-cuánticos sobre otros sistemas cuánticos, pero el verdadero poder de la nueva computación comenzó a verse cuando el físico David Deutsch de la Universidad de Oxford, Inglaterra publicó en 1985 un trabajo teórico crucial en el que describía al computador cuántico.

Durante los 90´s, las teorías planteadas inician el camino de la práctica con los algoritmos y aplicaciones cuánticas y las nacientes maquinas capaces de ejecutar cálculos cuánticos. Para 1993 **Dan Simon** desde el departamento de investigación de Microsoft, surgió un problema teórico que demostraba la ventaja práctica que tendría un computador cuántico frente a uno tradicional. Comparó el modelo de probabilidad clásica con el modelo cuántico y sus ideas sirvieron como base para el desarrollo de algunos algoritmos futuros (como el Algoritmo de Shor). En este mismo año, **Charles Benett** trabajador del centro de investigación de IBM en Nueva York descubrió el teletransporte

cuántico y que abrió una nueva vía de investigación hacia el desarrollo de comunicaciones cuánticas.

Para 1994 – 1995 **Peter Shor** científico estadounidense de AT&T Bell Laboratories definió el algoritmo que lleva su nombre y que permite calcular los factores primos de números a una velocidad mucho mayor que en cualquier computador tradicional. Además su algoritmo permitiría romper muchos de los sistemas de criptografía utilizados actualmente. Su algoritmo sirvió para demostrar a una gran parte de la comunidad científica que observaba incrédula las posibilidades de la computación cuántica, que se trataba de un campo de investigación con un gran potencial. Además, un año más tarde, propuso un sistema de corrección de errores en el cálculo cuántico.

Durante 1996 **Lov Grover i**nventó el algoritmo de búsqueda de datos que lleva su nombre. Aunque la aceleración conseguida no es tan drástica como en los cálculos factoriales o en simulaciones físicas, su rango de aplicaciones es mucho mayor. Al igual que el resto de algoritmos cuánticos, se trata de un algoritmo probabilístico con un alto índice de acierto. En 1997 se iniciaron los primeros experimentos prácticos y se abrieron las puertas para empezar a implementar todos aquellos cálculos y experimentos que habían sido descritos teóricamente hasta entonces. El primer experimento de comunicación segura usando criptografía cuántica se realiza con éxito a una distancia de 23 Km. Además se realiza el primer teletransporte cuántico de un fotón.

Entre 1998 – 1999 los investigadores de Los Álamos y el Instituto Tecnológico de Massachusets consiguen propagar el primer Qbit a través de una solución de aminoácidos. Supuso el primer paso para analizar la información que transporta un Qbit. Durante ese mismo año, nació la primera máquina de 2-Qbit, que fue presentada en la Universidad de Berkeley, California. Un año más tarde, en 1999, en los laboratorios de IBM-Almaden, se creó la primera máquina de 3-Qbit y además fue capaz de ejecutar por primera vez el algoritmo de búsqueda de Grover.

En el siglo XXI crecen los progresos, para el año 2000 de nuevo IBM, dirigido por I**saac Chuang** creó un computador cuántico de 5-Qbit capaz de ejecutar un algoritmo de búsqueda de orden, que forma parte del Algoritmo de Shor. Este algoritmo se ejecutaba en un simple paso cuando en un computador tradicional requeriría de numerosas iteraciones. Ese mismo año, científicos de Los Álamos National Laboratory anunciaron el desarrollo de un

computador cuántico de 7-Qbit. Utilizando un resonador magnético nuclear se consiguen aplicar pulsos electromagnéticos y permite emular la codificación en bits de los computadores tradicionales.

En el 2001 IBM y la Universidad de Stanford, consiguen ejecutar por primera vez el algoritmo de Shor en el primer computador cuántico de 7-Qbit desarrollado en Los Álamos. En el experimento se calcularon los factores primos de 15, dando el resultado correcto de 3 y 5 utilizando para ello 1018 moléculas, cada una de ellas con 7 átomos. Durante el 2005 el Instituto de "Quantum Optics and Quantum Information" en la universidad de Innsbruck (Austria) anunció que sus científicos habían creado el primer Qbyte, una serie de 8 Qbits utilizando trampas de iones. Para el 2006 los Científicos en Waterloo y Massachusetts diseñan métodos para mejorar el control del cuanto y consiguen desarrollar un sistema de 12-Qbits. El control del cuanto se hace cada vez más complejo a medida que aumenta el número de Qbits empleados por los computadores.

La empresa canadiense D-Wave Systems había supuestamente presentado el 13 de febrero de 2007 en Silicon Valley, una primera computadora cuántica comercial de 16-qubits de propósito general, luego la misma compañía admitió que tal máquina, llamada Orion, no es realmente una computadora cuántica, sino una clase de máquina de propósito general que usa algo de mecánica cuántica para resolver problemas. En ese mismo año para septiembre, dos equipos de investigación estadounidenses, el National Institute of Standards (NIST) de Boulder y la Universidad de Yale en New Haven consiguieron unir componentes cuánticos a través de superconductores. De este modo aparece el primer bus cuántico, y este dispositivo además puede ser utilizado como memoria cuántica, reteniendo la información cuántica durante un corto espacio de tiempo antes de ser transferido al siguiente dispositivo.

Para el 2008 la Fundación Nacional de Ciencias (NSF) de los EEUU, un equipo de científicos consiguió almacenar por primera vez un Qubit en el interior del núcleo de un átomo de fósforo, y pudieron hacer que la información permaneciera intacta durante 1.75 segundos. Este periodo puede ser expansible mediante métodos de corrección de errores, por lo que es un gran avance en el almacenamiento de información. El equipo de investigadores estadounidense dirigido por el profesor **Robert Schoelkopf,** de la universidad de Yale, que ya en 2007 había desarrollado el Bus cuántico, crea en el en el 2009 el primer procesador cuántico de estado sólido, mecanismo que funciona

de forma similar a un microprocesador convencional, aunque con la capacidad de realizar sólo unas pocas tareas muy simples, como operaciones aritméticas o búsquedas de datos. Para la comunicación en el dispositivo, esta se realiza mediante fotones que se desplazan sobre el bus cuántico, circuito electrónico que almacena y mide fotones de microondas, aumentando el tamaño de un átomo artificialmente.

Se encuentra que para el 2010 Investigadores del Centro de Tecnología de Computación Cuántica (CQTC) de la Universidad de Nueva Gales del Sur han logrado crear un transistor formado por siete átomos de fósforo. Los científicos han podido sustituir átomos individuales de un cristal de silicio por átomos de fósforo, formando un transistor que ocupa sólo 4 nanómetros. De igual manera, Un equipo de investigadores del Consejo Superior de Investigaciones Científicas (CSIC), junto a la Fundación Ikerbasque y el Instituto Walter-Meissner de Munich (Alemania), ha desarrollado un circuito cuántico que interacciona con las ondas electromagnéticas de forma más fuerte que cualquier material convencional, en un fenómeno conocido como "acoplo ultrafuerte" este circuito se fabrica con aluminio, material que a muy bajas temperaturas es superconductor", cable aclarar que existen dos tipos de circuitos cuánticos uno son elementos muy pequeños que se comportan como átomos y el segundo largos cables superconductores capaces de transportar microondas.

CRIPTOGRAFÍA CUÁNTICA

Uno de los grandes aportes que se han obtenido de la Computación Cuántica ha sido la Criptografía Cuántica propuesta en la década de 1970 pero en 1984 se publica su primer protocolo. Genera una nueva área dentro de la criptografía cumpliendo con los estándares de seguridad y protección de la información, brindando nuevas representaciones en la encriptación de datos, más fiables y sensibles a terceros dentro del proceso de la comunicación.

Unos de los principios de la física cuántica dicta que al medir un sistema cuántico se altera su contenido, es decir, en el instante que se trate de medirlo se está alterando de alguna manera, siendo esta característica el soporte de la Criptografía Cuántica debido a que si un agente externo de la comunicación intenta acceder sin permiso la información automáticamente se destruye.

"La seguridad de la criptografía cuántica reposa en los fundamentos de la mecánica cuántica, a diferencia de la criptografía de clave pública tradicional la cual descansa en supuestos de complejidad computacional no demostrada por ciertas funciones matemáticas. La criptografía cuántica se halla en las puestas de una producción masiva, utilizando láseres para emitir información en el elemento constituyente de la luz, el fotón, y conduciendo esta información a través de fibras ópticas".

CONCLUSIONES

La computación cuántica, se sustenta bajo una amplia gama de campos, es un tema bastante vasto que requiere una fuerte fundamentación teórica para ser tratado desde cualquier punto de vista.

Las aplicaciones, modelos y prototipos actuales que se desarrollan bajo el patrón de la computación cuántica, están en crecimiento, pero nos avecina a una posible nueva era de la humanidad.

La trascendencia de la computación cuántica radica en su aproximación a desarrollar capacidades infinitas de almacenamiento.

La complejidad de trabajar con escalas de nanos y unidades de Qubits, presenta también problemas para una óptima implementación de un ordenador cuántico, a pesar de que resuelve otros.

La computación cuántica es uno de los temas actuales más prometedores para el desarrollo de la tecnología y con una gran cantidad de áreas aplicables, que podrían hacer más entendible el comportamiento del universo.

Los aportes que la computación cuántica ha realizado al campo tecnología y al conocimiento han contribuido notablemente al desarrollo de nuevos conceptos como lo son la Criptografía Cuántica y la Comunicación Cuántica, mostrando al mundo dos concepciones mejoradas y con gran potencial para explotar.

Una de las grandes ventajas que nos ofrece la Computación Cuántica es aumento en la velocidad de procesamiento de la Información, pues al tener más capacidad de información y extraordinario poder de ejecución de un numero amplio de sentencias evidencian las limitaciones de la computación clásica en el desarrollo de tareas que anteriormente solo existían en la imaginación de los científicos.

BIBLIOGRAFÍA

Computación Cuántica, Sergi Baila Martinez. Consultado por última vez el 26 de Marzo de 2011 en:
http://fitxers.sargue.net/fitxers/quantum-es.pdf

Computación cuántica, Nasser Darwish Miranda. Universidad de La Laguna. Consultado por última vez el 26 de Marzo de 2011 en:
http://www.fceia.unr.edu.ar/~diazcaro/QC/Tutorials/Computacion%20Cuantica.pdf

Grupo de investigación en computación cuántica, Consultado por última vez el 26 de Marzo de 2011 en:
http://www.fceia.unr.edu.ar/~diazcaro/QC/Tutorials/Grupos%20de%20investigacion%20en%20Computacion%20Cuantica.pdf

SCIENCE AND SOCIETY: El Ordenador Insuperable, David Deutsch. Consultado por última vez el 26 de Marzo de 2011 en:
http://www.project-syndicate.org/commentary/deutsch1/Spanish

Google (2011). Historia de Computación Cuántica. Consultado por última vez el 27 de Marzo de 2011 en:
http://www.google.com/search?sourceid=chrome&ie=UTF-8&q=cuantico#q=historia+de+la+computaci%C3%B3n+cuantica&hl=es&sa=X&tbs=tl:1,tl_num:50&prmd=ivns&ei=d6ePTeLAOcK5tgeEkriICQ&ved=0CJADEMsBKAM&fp=1dc03753f060b83e

Wikipedia (2011). Computación Cuántica. Consultado por última vez el 27 de Marzo de 2011 en:
http://es.wikipedia.org/wiki/Computaci%C3%B3n_cu%C3%A1ntica

Textos Científicos (2011). Criptografía Cuántica. Consultado por última vez el 27 de Marzo de 2011 en:
http://www.textoscientificos.com/criptografia/quantica