Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

COMPUTACIÓN CUÁNTICA

Byron Rolando Cifuentes Pérez

Asesorado por el Ing. Calixto Raúl Monzón Pérez

Guatemala, octubre de 2006

UNIVERSIDAD DE SAN CAROLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

COMPUTACIÓN CUÁNTICA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

BYRON ROLANDO CIFUENTES PÉREZ

ASESORADO POR EL ING. CALIXTO RAÚL
MONZÓN PÉREZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2006

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paíz Recinos
VOCAL I	Inga. Glenda Patricia Garcia Soria
VOCAL II	Lic. Amahán Sánchez Alvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Jorge Armin Mazariegos Rabanales
EXAMINADOR	Ing. Otto Amilcar Rodríguez Ordoñez
EXAMINADOR	Ing. Rolando Aroldo Alanzo Ordoñez
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

COMPUTACIÓN CUÁNTICA,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha junio de 2005.

Byron Rolando Cifuentes Pérez

AGRADECIMIENTOS A:

DIOS Y LA VIGEN MARÍA	Por concederme un logro más en la vida.
EN ESPECIAL A MIS PADRES	MARTA LIDIA Y REGINALDO, por todo su esfuerzo, apoyo y todo el amor que me brindan, los amo mucho.
MI ESPOSA	JENNY JUDITH CHACON FRANCO, por todo el apoyo, entusiasmo y motivación que me brindaste, gracias mi amor.
MI HIJO	BYRON JOSE, por la motivación para poder predicar con el ejemplo.
MIS HERMANOS	GUISELA ,ERICK y AMILCAR, por todo el apoyo que me brindaron.
MI TÍO	ROCAEL, por todo el apoyo y los conocimientos que me brindó.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

GLOSARIO

Bit Unidad de medida de la capacidad de memoria equivalente a la posibilidad de almacenar la selección entre dos posibilidades, especialmente, usado en los computadores.

Criptografía Método por el cual se logra cifra o descifras mensajes

Electrón Dentro de la transmisión eléctrica, la unidad se denomina electrón

Foton Dentro del sistema óptico, la unidad óptica se denomina fotón

HBT Heterojuction Bipolar Transistor (Bipolar de Hetereoestructura)

HEMT Hight Electron Mobility Transistor (De Alta Movilidad).

JFET llamado transistor unipolar

ket Es un descriptor de un sistema cuántico en un instante de tiempo.

MESFET transistores de efecto de campo metal semiconductor.

MOSFET transistores de efecto de campo de metal-oxido semiconductor

QBit Unidad de medida de la capacidad de memoria equivalente a la posibilidad de almacenar de la computadora cuántica

RESUMEN

La idea base para la computación cuántica es muy sencilla, pero como siempre de la cosas simples se desprende un gran cúmulo de sabiduría.

El trabajo se divide en 4 capítulos, el primero aunque suene aburrido por ser un recuento de los que tuvo que pasar dentro de la historia desde el ábaco hasta la computadora actual y sus componentes, tanto internos como externos, nos centra en lo que veremos en los capítulos siguientes.

El capítulo 2 es un resumen de los estudios y los conceptos generales ya aplicados dentro de la computación cuántica, así como de los aspectos relevantes antes de llegar a la construcción de la computadora cuántica.

El capítulo 3 es ya en si los aspectos mas relevantes a tomar en cuenta para la construcción de la computadora en si, tanto aspectos como las posibles forma con la tendencias actuales para llegar a la creación de la maquina mas potente de nuestros años.

Y, para finalizar, el capítulo 4, es ya una aplicación en la cual se puede desarrollar muy bien la computación cuántica y por la cual muchos pueden estas interesados en que este concepto se lleve a un término muy feliz y mas cercano de lo que los vemos ahora, la criptología que no es mas que la ciencia de enviar mensajes en clave para que no sean descifrados con facilidad.

OBJETIVOS

General

Que se dé a conocer los conceptos y los avances de la computación cuántica dentro del medio Guatemalteco.

Específicos

1. Poder tener un curso dentro de la universidad en el cual se impartan estos conceptos a todos los estudiantes de Ingeniería en sistemas.

2. Desarrollo de la teoría matemática que tiene las propiedades de la computación cuántica, para, así, contar con las herramientas para el desarrollo de nuevos algoritmos basados en esta nueva tecnología

3. Mostrar una nueva metodología para la resolución de problemas de procesamiento paralelo masivo a través de un enfoque de computación cuántica

ALCANCES

Se definirán todos los aspectos teóricos para la explicación de la computación cuántica que están hasta este momento validos, debido a que, según las investigaciones avanzan, los conceptos pueden cambiar.

Se presentarán los algoritmos más relevantes que hicieron que la computación cuántica se pueda empezar a definir, por ejemplo, el algoritmo de Short, así como la lógica cuántica de las operaciones básicas lógicas aplicada a la computación cuántica.

Se presentarán las diferentes modalidades de poder llegar a usar y construir un computador cuántico, dentro de los marcos teóricos actuales, pues, según los cambios que surjan, estos podrán cambiar.

INTRODUCCIÓN

¿Qué es Computación Cuántica?

Es una corriente que se esta propagando dentro de las nuevas investigación, con el objetivo de poder hacer que las maquinas puedan resolver en un tiempo menor los problemas.

Con este tipo de investigación se logra fusionar dos teorías que están luchando por mantenerse una y sobresalir la otra, la física clásica y la física cuántica, los conceptos de una y otra hicieron nacer primero el concepto de Computación normal y ahora con los nuevos conceptos aplicados a la computación de la física cuántica surge la computación quántica.

La computación cuántica se empezó a estudiar a raíz, entre otras, de una propuesta de Richard Feynman (1982), motivada por el alto coste computacional que exige el cálculo de la evolución de sistemas cuánticos.

Él sugirió considerar la evolución de los sistemas cuánticos no como objetos a calcular sino como herramientas de cálculo, es decir, como ordenadores. El área se desarrolló lentamente hasta que Peter W. Shor sorprendió a todos, en 1994, describiendo un algoritmo polinomial para factorizar enteros. Este descubrimiento generó una gran actividad que ha provocado un desarrollo vertiginoso del área.

Clásicamente el tiempo que cuesta realizar cálculos se puede reducir usando procesadores en paralelo. Para alcanzar una reducción exponencial es necesario un número exponencial de procesadores y por tanto una

cantidad exponencial de espacio físico. Sin embargo, en sistemas cuánticos la capacidad de cálculo en paralelo crece, exponencialmente, respecto al espacio requerido por el sistema. Este efecto se llama paralelismo cuántico.

1 MARCO TEÓRICO

1.1 Conceptos Básicos de Física o Mecánica Clásica

Dentro de los conceptos que tocaremos para poder definir la física clásica, no serán conceptos como vectores o fuerza y velocidad, si no los conceptos básicos aplicados al desarrollo de las computadoras, los conceptos a los que nos referimos son tales como magnetismo, microcircuitos y las interfaces ópticas, utilizados en los disco ópticos la fibra óptica, etc.

La física en si se divide realmente en dos áreas teóricas, la mecánica y la termodinámica, los de mas son conceptos aplicado de esta, como por ejemplo la mecánica de fluidos, el electromagnetismo, la electrónica, la acústica, la física molecular, atómica y nuclear, la óptica, la química física, la física del estado sólido, etc. Todas ellas se fundamentan en la mecánica (clásica y cuántica) y la termodinámica.

La mecánica teórica, tanto la clásica como la cuántica, trata exclusivamente de la comprensión del principio de la conservación de la energía. Este es el primer principio fundamental de la física, que permite explicar un gran número de propiedades de la naturaleza. En otras palabras, la mecánica nos enseña a comprender y a operar con el principio de la conservación de la energía.

La distinción entre mecánica clásica y mecánica cuántica reside en su ámbito de aplicación. Hasta que no se investigó la naturaleza íntima de la materia (su naturaleza atómica y subatómica), la formulación de la mecánica clásica era suficiente para la descripción de los fenómenos conocidos. Al empezar a investigar los fenómenos atómicos, se izo patente que la mecánica clásica era insuficiente para este campo de investigación. La mecánica cuántica surge para solventar este problema, de modo que la mecánica clásica queda incluida en la mecánica cuántica. La mecánica cuántica coincide con la mecánica clásica cuando se aplica a sistemas superiores al nuclear, es decir, a sistemas de escala natural o humana.

La termodinámica tiene un nivel de integración teórica superior, puesto que trata de la comprensión del principio del incremento de la entropía y de su interrelación con el principio de la conservación de la energía (llamados respectivamente segundo principio y primer principio de la termodinámica). Por tanto, el análisis termodinámico integra la aplicación de los dos principios fundamentales de la física (incluye, por tanto, a la mecánica).

Para los biólogos, la termodinámica es el nivel de análisis físico que nos interesa, puesto que, como veremos, en los seres vivos, tan importantes son las consecuencias del principio de la conservación de la energía, como las del principio del incremento de la entropía. Es decir, no nos basta con una comprensión adecuada de la mecánica sino que debemos alcanzar también una comprensión adecuada de la termodinámica.

1.2 Introducción a la Ciencia de la computación

Las computadoras en la actualidad, aun funcionan con los microcircuitos, el magnetismo, el cual ya esta por salir y ser desplazado por los mecanismos ópticos o luz.

Durante los años las computadoras han estado relacionadas con lo que son las matemáticas y lo estados de la física clásica, estos conceptos se han ido reforzando con los años, empezando con lo que es el ábaco, luego las calculadoras, y muchos artefactos mas, de los cuales explicaremos los conceptos básicos de los mas relevantes para la computación.

1.3 Marco histórico de las computadoras

Por toda la historia, el desarrollo de máquinas matemáticas ha ido de mano en mano con el desarrollo de computadoras. Cada avance en uno es seguido inmediatamente por un avance en el otro. Cuando la humanidad desarrolló el concepto del sistema de conteo en base diez, el abacus fue una herramienta para hacerlo más fácil. Cuando las computadoras electrónicas fueron construidas para resolver ecuaciones complejas, campos como la dinámica de fluidos, teoría de los números, y la física química floreció.

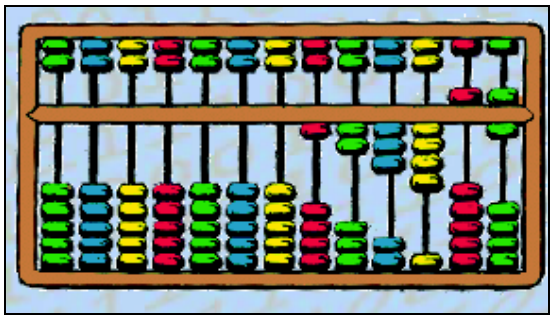
1.3.4 500 a.C. - 1822 d.C.

Esta comienza desde la aparición del abacus en China y Egipto, alrededor de 500 años a.C. hasta la invención del Motor Diferencial por Charles Babbage, en 1822. El descubrimiento de los sistemas por Charles Napier, condujo a los avances en calculadoras. Por convertir multiplicación y división en suma y resta, un número de máquinas (incluyendo la regla deslizante) puede realizar estas operaciones. Babbage sobrepasó los límites de la ingeniería cuando inventó su motor, basado en este principio.

1.3.5 El ábaco

El ábaco fue la primera máquina conocida que ayudaba a ejecuta computaciones matemáticas. Se piensa que se originó entre 600 y 500 a.C., o en China o Egipto. Pelotas redondas, usualmente de madera, se resbalaban de un lado a otro en varas puestas o alambres, ejecutaban suma y substracción. Como una indicación de su potencial, se usa el ábaco todavía en muchas culturas orientales hoy en día.

Figura 1 Ábaco



1.3.6 Napier Bones

Justo antes de morir en 1617, el matemático escocés John Napier (mejor conocido por su invención de logaritmos) desarrolló un juego de palitos para calcular a las que llamó "Napier Bones." Así llamados porque se tallaron las ramitas de hueso o marfil, los "bones" incorporaron el sistema logarítmico. Los Huesos de Napier tuvieron una influencia fuerte en el desarrollo de la regla deslizante (cinco años más tarde) y máquinas calculadoras subsecuentes que contaron con logaritmos.

1.3.7 Calculadora mecánica

En 1623 la primera calculadora mecánica fue diseñada por Wilhelm Schickard en Alemania. Llamado "El Reloj Calculador", la máquina incorporó los logaritmos de Napier, hacia rodar cilindros en un albergue grande. Se comisionó un Reloj Calcualdor para Johannes Kepler, el matemático famoso, pero fue destruido por fuego antes de que se terminara.

1.3.8 Pascalina

En 1642 la primera calculadora automática mecánica fue inventada por el matemático francés y filósofo Blaise Pascal. Llamado la "Pascalina", el aparato podía multiplicar y substraer, utilizando un sistema de cambios para pasar dígitos. Se desarrolló la máquina originalmente para simplificar al padre de Pascal para la recolección del impuesto. Aunque el Pascalina nunca fue un éxito comercial como Pascal había esperado, el principio de los cambios era fue útil en generaciones subsecuentes de calculadoras mecánicas.

1.3.9 La máquina de multiplicar

En 1666 la primera máquina de multiplicar se inventó por Sir Samuel Morland, entonces Amo de mecánicas a la corte de Rey Charles II de Inglaterra. El aparato constó de una serie de ruedas, cada representaba, dieses, cientos, etc. Un alfiler del acero movía los diales para ejecutar las calculaciones. A diferencia de la Pascalina, el aparato no tenía avanzó automático de en columnas.

1.3.10 Máquina calculadora

La primera calculadora de propósito general fue inventada por el matemático alemán Gottfried von Leibniz en 1673. El aparato era una partida de la Pascalina, mientras opera usa un cilindro de dientes (la rueda de Leibniz) en lugar de la serie de engranaje. Aunque el aparato podía ejecutar multiplicación y división, padeció de problemas de fiabilidad que disminuyeron su utilidad.

1.3.11 El jugador de ajedrez automático

En 1769 el Jugador de Ajedrez Autómata fue inventado por Barón Empellen, un noble húngaro. El aparato y sus secretos se le dieron a Johann Nepomuk Maelzel, un inventor de instrumentos musicales, quien recorrió Europa y los Estados Unidos con el aparato, a finales de 1700 y temprano 1800. Pretendió ser una máquina pura, el Autómata incluía un jugador de ajedrez "robótico". El Autómata era una sensación dondequiera que iba, pero muchas comentaristas, incluso el Edgar Allen Poe famoso, ha escrito críticas detalladas diciendo que ese era una "máquina pura." En cambio, generalmente, siempre se creyó que el aparato fue operado por un humano oculto en el armario debajo del tablero de ajedrez. El Autómata se destruyó en un incendio en 1856.

1.3.12 La máquina lógica

Se inventó la primera máquina lógica en 1777 por Charles Mahon, el Conde de Stanhope. El "demostrador lógico" era un aparato tamaño bolsillo que resolvía silogismos tradicionales y preguntas elementales de probabilidad. Mahon es el precursor de los componentes lógicos en computadoras modernas.

1.3.13 Jacquard Loom

El "Jacquard Loom" se inventó en 1804 por Joseph-Marie Jacquard. Inspirado por instrumentos musicales que se programaban usando papel agujereados, la máquina se parecía a una atadura del telar que podría controlar automáticamente de dibujos usando una línea tarjetas agujereadas. La idea de Jacquard, que revolucionó el hilar de seda, estaba formar la base de muchos aparatos de la informática e idiomas de la programación.

1.3.14 Calculadoras de producción masiva

La primera calculadora de producción masiva se distribuyó, empezando en 1820, por Charles Thomas de Colmar. Originalmente se les vendió a casas del seguro Parisienses, el "aritmómetro" de Colmar operaba usando una variación de la rueda de Leibniz. Más de mil aritmómetro se vendieron y eventualmente recibió una medalla a la Exhibición Internacional en Londres en 1862.

1.3.15 Artefacto de la diferencia

En 1822 Charles Babbage completó su "Artefacto de la Diferencia," una máquina que se puede usar para ejecutar calculaciones de tablas simples. El Artefacto de la Diferencia era una asamblea compleja de ruedas, engranajes, y remaches. Fue la fundación para Babbage diseñar su "Artefacto Analítico," un aparato del propósito genera que era capaz de ejecutar cualquiera tipo de calculación matemática. Los diseños del artefacto analítico eran la primera conceptualización clara de una máquina que podría ejecutar el tipo de computaciones que ahora se consideran al corazón de informática. Babbage nunca construyó su artefacto analítico, pero su plan influyó en toda computadora moderna digital que estaba a seguir. Se construyó el artefacto analítico finalmente por un equipo de ingenieros en 1989, cien años después de la muerte de Babbage en 1871. Por su

discernimiento Babbage hoy se sabe como el "Padre de Computadoras Modernas".

1.3.16 1823 - 1936

Durante este tiempo, muchas de las culturas del mundo fueron avanzando desde sociedades basadas en la agricultura a sociedades basadas industrialmente. Con estos cambios vinieron los avances matemáticos y en ingeniería los cuales hicieron posible máquinas electrónicas que pueden resolver argumentos lógicos complejos. Comenzando con la publicación de Boolean Algebra de George Boole y terminando con la fabricación del modelo de la Máquina de Turín para máquinas lógicas, este período fue muy próspero para computadoras.

En esta etapa se inventaron las siguientes:

1.3.16 Algebra de Boole

En 1854 el desarrollo del Algebra de Boolean fue publicado por el lógico Inglés George S. Boole. El sistema de Boole redujo argumentos lógicos a permutaciones de tres operadores básicos algebraicos: "y", "o", y "'no". A causa del desarrollo de el Algebra de Boolean, Boole es considerado por muchos ser el padre de teoría de la información.

1.3.17 Máquina lógica de Boolean

En 1869 la primera máquina de la lógica a usar el Algebra de Boolean para resolver problemas más rápido que humanos, fue inventada por William Stanley Jevons. La máquina, llamada el Piano Lógico, usó un alfabeto de cuatro términos lógicos para resolver silogismos complicados.

1.3.18 Calculadora guiada por teclas

En 1885 la primera calculadora guiada por teclas exitosas, se inventó por Dorr Eugene Felt. Para preservar la expansión del modelo del aparato, llamado el "Comptómetro", Felt compró cajas de macarrones para albergar los aparatos. Dentro de los próximos dos años Felt vendió ocho de ellos al New York Weather Bureau y el U.S. Tresury. Se usó el aparato principalmente por contabilidad, pero muchos de ellos fueron usados por la U.S. Navy en computaciones de ingeniería, y era probablemente la máquina de contabilidad más popular en el mundo en esa época.

1.3.19 Sistema de tarjetas agujeradas

En 1886 la primera máquina tabuladora en usar una tarjeta agujerada de entrada del datos fue inventado por Dr. Herman Hollerith. Fue desarrollada por Hollerith para usarla en clasificar en 1890 el censo en U.S., en que se clasificó una población de 62,979,766. Su ponche dejó que un operador apuntara un indicador en una matriz de agujeros, después de lo cual se picaría en una tarjeta pálida un agujero al inverso de la máquina. Después del censo Hollerith fundó la Compañía de las Máquinas de Tabulación, que, fusionando adquiere otras compañías, llegó a ser qué es hoy Máquinas del Negocio Internacionales (IBM).

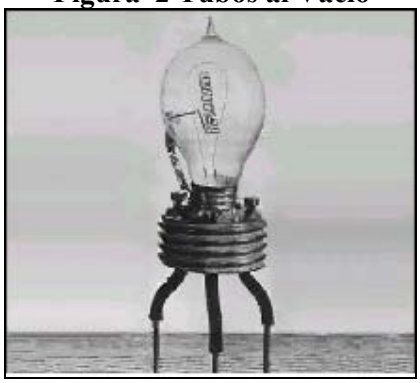
1.3.20 Máquina de multiplicar

En 1893 la primera máquina exitosa de multiplicación automática se desarrolló por Otto Steiger. "El Millonario," como se le conocía, automatizó la invención de Leibniz de 1673, y fue fabricado por Hans W. Egli de Zurich. Originalmente hecha para negocios, la ciencia halló inmediatamente un uso para el aparato y varios miles de ellos se vendieron en los cuarenta años que siguió.

1.3.21 Tubo al vacío

En 1906 el primer tubo al vacío fue inventado por un inventor americano, Lee De Forest. "El Audion", como se llamaba, tenía tres elementos dentro de una bombilla del vidrio evacuada. Los elementos eran capaces de hallar y amplificar señales de radio recibidas de una antena. El tubo al vacío encontraría uso en varias generaciones tempranas de computadoras, a comienzos de 1930.

Figura 2 Tubos al Vació



Tubos de vacío o Válvulas de vacío, dispositivos electrónicos que consisten en una cápsula de vacío de acero o de vidrio, con dos o más electrodos entre los cuales pueden moverse libremente los electrones. El diodo de tubo de vacío fue desarrollado por el físico inglés John Ambrose Fleming. Contiene dos electrodos: el cátodo, un filamento caliente o un pequeño tubo de metal caliente que emite electrones a través de emisión termoiónica, y el ánodo, una placa que es el elemento colector de electrones. En los diodos, los electrones emitidos por el cátodo son atraídos por la placa sólo cuando ésta es positiva con respecto al cátodo. Cuando la placa está cargada negativamente, no circula corriente por el tubo. Si se aplica un potencial alterno a la placa, la corriente pasará por el tubo solamente durante la mitad positiva del ciclo, actuando así como rectificador. Los diodos se emplean en la rectificación de corriente alterna. La introducción de un tercer electrodo, llamado rejilla, interpuesto entre el cátodo y el ánodo, forma un triodo, que ha sido durante muchos años el tubo

base utilizado para la amplificación de corriente. El triodo fue inventado por el ingeniero estadounidense Lee De Forest en 1906. La rejilla es normalmente una red de cable fino que rodea al cátodo y su función es controlar el flujo de corriente. Al alcanzar un potencial negativo determinado, la rejilla impide el flujo de electrones entre el cátodo y el ánodo.

Con potenciales negativos más bajos el flujo de electrones depende del potencial de la rejilla. La capacidad de amplificación del triodo depende de los pequeños cambios de voltaje entre la rejilla y el cátodo, que a su vez causan grandes cambios en el número de electrones que alcanzan el ánodo. Con el paso del tiempo se han desarrollado tubos más complejos con rejillas adicionales que proporcionan mayor amplificación y realizan funciones específicas. Los tetrodos disponen de una rejilla adicional, próxima al ánodo, que forma una barrera electrostática entre el ánodo y la rejilla. De esta forma previene la realimentación de la misma en aplicaciones de alta frecuencia. El pentodo dispone de tres rejillas entre el cátodo y el ánodo; la tercera rejilla, la más próxima al ánodo, refleja los electrones emitidos por el ánodo calentado por los impactos electrónicos cuando la corriente de electrones en el tubo es elevada. Los tubos con más rejillas, denominados hexodos, heptodos y octodos, se usan como convertidores y mezcladores de frecuencias en receptores de radio.

Prácticamente la totalidad de los tubos de vacío han sido reemplazados por transistores, que son más baratos, económicos y fiables. Los tubos todavía desempeñan un papel importante en determinadas aplicaciones, como las etapas de potencia de los transmisores de radio y televisión o en equipos militares que deben resistir el pulso de voltaje inducido por las explosiones nucleares atmosféricas, que destruyen los transistores

Los microcircuitos o Transistores

1.3.22 Flip-flop

En 1919 el primero circuito multivibrador bistable (o flip-flop) fue desarrollado por inventores americanos W.H. Eccles y F.W. Jordan. El flip-flop dejó que un circuito tuviera uno de dos estados estables, que estaban intercambiable. Formó la base por el almacenamiento del bit binario estructura de computadoras de hoy.

1.3.23 Computadora analógica (para ecuaciones diferenciales)

En 1931 la primera computadora capaz de resolver ecuaciones diferenciales analógicos fue desarrollada por el Dr. Vannevar Bush y su grupo de investigación en MIT. "El Analizador Diferencial", como se llamaba, usaba engranajes diferenciales que fueron hechos rodar por motores eléctricos. Se interpretaron como cantidades los grados de rotación de los engranajes. Computaciones fueron limitadas por la precisión de medida de los ángulos.

1.3.24 Programa mecánico

En 1933 el primer programa mecánico fue diseñado por Wallace J. Eckert. El programa controló las funciones de dos de las máquinas en unísono y operadas por un cable. Los trabajos de Eckert sembraron la fundación para las investigaciones informático-científica de la Universidad de Colombia.

1.3.25 Máquina lógica

En 1936 el primer modelo general de máquinas de la lógica fue desarrollado por Alan M. Turing. El papel, tituló "En Números calculables," se

publicó en 1937 en la Sociedad de Procedimientos Matemáticos de Londres y describió las limitaciones de una computadora hipotética. Números calculables eran esos números que eran números reales, capaz de ser calculados por medios del lo finito. Turing ofreció prueba que mostró que al igual cuando usa un proceso finito y definido por resolver un problema, problemas seguros todavía no se pueden resolver. La noción de las limitaciones de tal problema tiene un impacto profundo en el desarrollo futuro de ciencia de la computadora.

1.3.26 1937 - 1949

Durante la segunda guerra mundial, estudios en computadoras fueron de interés nacional. Un ejemplo de ello es el "Coloso", la contra inglés a la máquina Nazi de códigos, el "Enigma". Después de la guerra, el desarrollo empezó su nido, con tecnología eléctrica permitiendo un avance rápido en computadoras.

En esta etapa se inventaron las siguientes:

1.3.27 Las funciones de cambio

En 1937 Claude F. Shannon dibujó el primer paralelo entre la Lógica de Boolean y cambió circuitos en la tesis del patrón en MIT. Shannon siguió desarrollando sus teorías acerca de la eficacia de la información comunicativa. En 1948 formalizó estas ideas en su "teoría de la información," que cuenta pesadamente con la Lógica de Boolean.

1.3.28 Electrónica digital

En 1939 la primera computadora electrónica digital se desarrolló en la Universidad del Estado de Iowa por Dr. John V. Atanasoff y Clifford Baya. El prototipo, llamó el Atanasoff Berry Computer (ABC), fue la primera máquina en hacer uso de tubos al vacío como los circuitos de la lógica.

1.3.29 Computadora programable

En 1941 la primera controladora para computadora para propósito general usada se construyó por Konrad Zuse y Helmut Schreyer. El "Z-3," como se llamó, usaba retardos electromagnéticos y era programada usando películas agujereadas. su sucesor, el "Z-4," fue contrabandeado fuera de Berlín cuando Zuse escapo de los Nazis en Marzo de 1945.

1.3.30 El magnetismo

La piedra de magnesia o imán, como diríamos actualmente, ya era conocida en la antigüedad. Efectivamente, la magnes lithos, tal como la llamaban los griegos, era una piedra de imán originaria de Magnesia de Sílilo, una ciudad griega de Lidia, fundada en el siglo III de nuestra era, y que hoy día lleva el nombre de Manisa y se encuentra en la actual Turquía. Se trataba de una región donde se hallaban en abundancia estos famosos imanes, cuyas propiedades conocieron los griegos desde el siglo VI, antes de Jesucristo. En efecto, el astrónomo, matemático y filósofo griego Tales de Mileto fue el primero en hacer una clara descripción de ellos. Señalemos de paso que aunque se concede el título de astrónomo a este sabio de la antigüedad, no podemos excluir la hipótesis de que fuera astrólogo. Este sabio tuvo la idea de determinar la altura de un objeto a partir de su sombra y se le atribuye la previsión de un eclipse de Sol en el año 585 antes de nuestra era.

Figura 3 Iman

Solamente a partir del siglo XI de nuestra era, la piedra de magnesia se utilizó para construir un instrumento de navegación, la brújula, que funciona gracias a una aguja imantada. Sin embargo, fue a de finales del siglo XVIII que se emprendió el estudio cuantitativo del magnesio. En esta época en que, por una parte, Charles de Coulombo (1736-1806), un físico francés de la primera promoción de científicos modernos, por decirlo de alguna manera, exponía ante la Academia de Ciencias las bases experimentales y teóricas del magnetismo y de la electroestática y época en que, por otra parte, un médico alemán llamado Franz Anton Mesmer (1734-1825) avanzaba la tesis de la existencia de un fluido magnético animal en el que veía un posible remedio a todas les enfermedades, tesis que fue refutada en 1843.

1.3.30.1 ¿Qué es el magnetismo?

El magnetismo es una fuerza invisible, sin embargo, su poder se manifiesta cuando un objeto metálico es atraído por un imán. El material que atrae ciertos metales, como el hierro, se llama magneto o imán. Los objetos que son atraídos se llaman magnéticos.

Los imanes poseen dos polos o masas magnéticas iguales y opuestas. Sin embargo, si se intenta aislar a uno de estos polos o una de estas dos masas, la corriente deja de pasar, el fenómeno de la imantación desaparece.

La brújula magnética funciona a partir de este principio. Está provista de una aguja de hierro que puede girar libremente y que, como arte de magia, parece atraída por el campo magnético terrestre, apuntando hacia el polo norte magnético de la Tierra, el cual se encuentra muy cerca del Polo Norte geográfico. Las brújulas se utilizan para orientarse tanto en el mar como en la tierra. Aunque este instrumento se utiliza normalmente en la navegación.

Tierra y magnetismo La Tierra es un imán, exactamente igual que aquellos de pequeño tamaño que a menudo se utilizan para colgar notas en la puerta del refrigerador. Pero es un imán tan grande que afecta al resto de los imanes del planeta. Si cuelgas de un hilo un imán alargado de tal forma que pueda girar libremente, uno de sus extremos girará siempre hasta apuntar hacia el Polo Norte, y el otro lo hará hacia el Polo Sur.

A ciencia cierta no se sabe bien por qué la Tierra es magnética. La mayoría de los imanes dejan de funcionar cuando se calientan; pues bien, la Tierra no, y esto a pesar de que su núcleo tiene calor suficiente como para fundir cualquier metal. Hoy en día, la mayor parte de los científicos creen que este magnetismo se debe a que dicho calor mantiene la parte exterior y fluida del núcleo terrestre en continuo movimiento.

El núcleo de la Tierra es rico en material magnético, y este movimiento circulatorio genera electricidad, al igual que un dínamo de bicicleta o en una central eléctrica. Son estas corrientes eléctricas las que hacen de la Tierra un imán gigante

1.3.31 Electrónica inglesa

En el diciembre de 1943 se desarrolló la primera calculadora inglesa electrónica para criptoanálisis. "El Coloso," como se llamaba, se desarrolló

como una contraparte al Enigma, La máquina codificación de Alemania. Entre sus diseñadores estaban Alan M. Turing, diseñador de la Máquina Turing, quien había escapado de los Nazis unos años antes. El Coloso tenía cinco procesadores, cada uno podría operar a 5,000 caracteres por segundo. Por usar registros especiales y un reloj interior, los procesadores podrían operar en paralelo (simultáneamente) que esta le daba al Coloso una rapidez promedio de 25,000 caracteres por segundo. Esta rapidez alta era esencial en el esfuerzo del desciframiento de códigos durante la guerra. El plan del Coloso era quedar como información secreta hasta muchos años después de la guerra.

1.3.32 Marca I ASCC

En 1944, el primer programa controlador americano para computadora fue desarrollado por Howard Hathaway Aiken. La "Calculadora Automática Controlada por Secuencia (ASCC) Marca I," como se llamaba, fue un parche de los planes de Charles Babbage por el artefacto analítico, de cien años antes. Cintas de papel agujereados llevaban las instrucciones. El Mark que midió cincuenta pies de largo y ocho pies de alto, con casi quinientas millas de instalación eléctrica, y se usó a la Universidad de Harvard por 15 años.

1.3.33 El primer error de computadora (bug)

El 9 de septiembre de 1945, a las 3: 45 pm, el primer caso real de un error que causa un malfuncionamiento en la computadora fue documentado por los diseñadores del Marca II. El Marca II, sucesor al ASCC Marca que se construyó en 1944, experimentó un falló. Cuando los investigadores abrieron caja, hallaron una polilla. Se piensa ser el origen del uso del término "bug" que significa insecto o polilla en inglés.

1.3.34 El ENIAC

En 1946 la primera computadora electrónica digital a grande escala llegó a ser operacional. ENIAC (Integrado Electrónico Numérico y Calculadora) usó un sistema de interruptores montados externamentes y enchufes para programarlo. El instrumento fue construido por J. Presper Eckert Hijo y John Mauchly. La patente por el ENIAC no fue aceptada, de cualquier modo que, cuando se juzgó como se derivó de una máquina del prototipo diseñado por el Dr John Vincent Atanasoff, quien también ayudó a crear la computadora Atanasoff-Berry. Se publicó trabajo este año que detalla el concepto de un programa guardado. Se completa sucesor a ENIAC, el EDVAC, en 1952.

1.3.35 El transistor

En 1947 se inventó la primera resistencia de traslado, (transistor) en Laboratorios Bell por John Bardeen, Walter H. Brattain, y William Shockley. Los diseñadores recibieron el Premio Nobel en 1956 por su trabajo. El transistor es un componente pequeño que deja la regulación del flujo eléctrico presente. El uso de transistores como interruptores habilitaron computadoras llegar a ser mucho más pequeño y subsiguientemente llevó al desarrollo de la tecnología de la "microelectrónica".

1.3.36 Qué son los Transistores:

Dispositivo semiconductor activo que tiene tres o más electrodos. Los tres electrodos principales son emisor, colector y base. La conducción entre estos electrodos se realiza por medio de electrones y huecos. El germanio y el sicilio son los materiales más frecuentemente utilizados para la fabricación de los elementos semiconductores. Los transistores pueden efectuar prácticamente todas las funciones de los antiguos tubos electrónicos, incluyendo la ampliación y la rectificación, con muchísimas ventajas

Elementos de un transistor o transistores:

El transistor es un dispositivo semiconductor de tres capas que consiste de dos capas de material tipo n y una capa tipo p, o bien, de dos capas de material tipo p y una tipo n. al primero se le llama transistor npn, en tanto que al segundo transistor pnp.

EMISOR, que emite los portadores de corriente,(huecos o electrones). Su labor es la equivalente al CATODO en los tubos de vacío o "lámparas" electrónicas.

BASE, que controla el flujo de los portadores de corriente. Su labor es la equivalente a la REJILLA cátodo en los tubos de vacío o "lámparas" electrónicas.

COLECTOR, que capta los portadores de corriente emitidos por el emisor. Su labor es la equivalente a la PLACA en los tubos de vacío o "lámparas" electrónicas

Ventajas de los transistores

- El consumo de energía es sensiblemente bajo.
- El tamaño y peso de los transistores es bastante menor que los tubos de vacío.
- Una vida larga útil (muchas horas de servicio).
- Puede permanecer mucho tiempo en deposito (almacenamiento).
- No necesita tiempo de calentamiento.
- Resistencia mecánica elevada.
- Los transistores pueden reproducir otros fenómenos, como la fotosensibilidad

Tipos de Transistores

Transistores Bipolares de unión, BJT. (PNP o NPN)

BJT, de transistor bipolar de unión (del ingles, Bipolar Junction Transistor).

El termino bipolar refleja el hecho de que los huecos y los electrones participan en el proceso de inyección hacia el material polarizado de forma opuesta.

Transistores de efecto de campo. (JFET, MESFET, MOSFET)

JFET, De efecto de campo de unión (JFET): Tambien llamado transistor unipolar, fué el primer transistor de efecto de campo en la práctica. Lo forma una barra de material semiconductor de silicio de tipo N o P. En los terminales de la barra se establece un contacto óhmico, tenemos así un transistor de efecto de campo tipo N de la forma más básica.

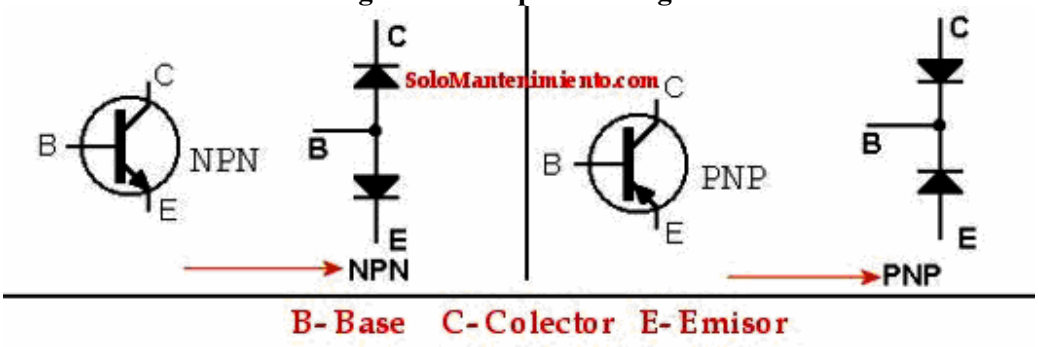
MESFET, transistores de efecto de campo metal semiconductor.

MOSFET, transistores de efecto de campo de metal-oxido semiconductor. En estos componentes, cada transistor es formado por dos islas de silicio, una dopada para ser positiva, y la otra para ser negativa, y en el medio, actuando como una puerta, un electrodo de metal.

Transistores HBT y HEMT

Las siglas HBT y HEMT pertenecen a las palabras Heterojuction Bipolar Transistor (Bipolar de Hetereoestructura) y Hight Electron Mobility Transistor (De Alta Movilidad). Son dispositivos de 3 terminales formados por la combinación de diferentes componentes, con distinto salto de banda prohibida

Figura 4 Compuertas Logias



1.3.37 La computadora "Guarda Programas"

En 1948 la primera computadora de guardado de programa se desarrolló en la Universidad Manchester por F.C . y Williams T. Kilburn. El "Manchester Marca I", como se llamaba, se construyó para probar un tubo CRT de la memoria, inventada por Williams. Como tal, era una computadora escala. Una computadora a gran escala de guardado de programas se desarrolló un año más tarde (EDSAC) por un equipo encabezado por Maurice V. Wilkes.

1.3.38 Memoria

En 1949 la primera memoria fue desarrollada por Jay Forrester. Empezando en 1953, la memoria, que constó de una reja de anillos magnéticos en alambre interconectados, reemplazó los no confiables tubos al vacío como la forma predominante de memoria por los próximos diez años.

1.3.39 Dispositivos Ópticos

La luz es uno de las ultimas formas usadas para ampliar espacios y mejorar la velocidad de repuesta, dentro de la computación, pero esta sigue siendo una forma de la física normal, como funcionan estos dispositivos lo definiremos en 2, la primera es para mejorar el espacio y la segunda para

mejorara la velocidad. Para mejorar el espacio se utiliza la luz con superficies mas planas y fáciles de poder quemar, son los CD's, los Mini Disk's que al final usan la misma tecnología de los CD's y los DVS los cuales son los dispositivos que por el momento tiene la mayor capacidad de almacenamiento. Estas son superficies que parecen espejos, en la cuales poner un uno o cero (1,0) no es mas que halla o no presencia de luz dentro del dispositivo.

Para mejorar la velocidad estamos halando de la fibra óptica la cual esta siendo usada para la transmisión de información desde un punto a otro por medio de señales de luz, o sea de nuevo un uno o cero (1,0) es la presencia o no presencia de luz dentro de dispositivo que estamos usando. Tanto los dispositivos de almacenamiento masivo y la fibra óptica han venido a revolucionar la ciencia de la computación, pues ahora ya se puede transportar mas información, ya se pueden hacer discos ópticos que capten y contengan mayor información, así como las velocidades de transmisión de información dentro de la fibra óptica ha superado las expectativas.

Pero al final siguen siendo solo o uno o cero, lo cual nos atrapa nuevamente en la física tradicional, de la cual estamos o tratado de superara o buscando nuevos modelos para poder mejorar y salir de esta barrera que tenemos por el momento y con ello superar la computación.

Todo esto, la física clásica y los dispositivos, tubos al vació, magnetismo, microcircuitos y los dispositivos ópticos, son lo que dan vida a la computación actual, los tubos al vació son el inicio, y luego pasamos a magnetismo y por ultimo estamos en la época ya casi desapareciendo el magnetismo, tanto de los microcircuito y de la óptica que esta empezando a ser parte esencial de la computación. Pero ya casi estamos en el tope de lo que puede dar la física clásica, pues las técnicas para construir circuitos integrados se acercan a sus límites, todo esto dado por la mecánica tradicional.

Como desde el principio las bases de la computación se ha basado en la leyes de la mecánica clásica. Y estas leyes ya han alcanzado los niveles mas avanzados de la microelectrónica moderna, y aunque pudiéramos hacer diseños mucho mas óptimos y con mejoras nunca vistas, estos se apoyaran en el modelo de puerta lógicas[1] convencionales, el cual ya tiene las limitantes de este modelo y no las podremos superar sin la computación cuantica.

1.3.40 Fibras ópticas

En la búsqueda por encontrar materiales conductores capaces de soportar transmisiones de altas frecuencias, resistentes a temperaturas variables y condiciones ambientales, los ingenieros y tecnologos desde mediados de siglo empezaron a desarrollar nuevas tecnologías de transmisión. Los cables de hierro que llevaban mensajes telegráficos no pueden soportar las frecuencias necesarias para acarrear a largas distancias las llamadas telefónicas sin pasar por severas distorsiones. Por ello las compañías telefónicas se movieron hacia los pares de cables de cobre. Aunque éstos cables trabajaron y continúan trabajando bien en algunas redes, para los años cincuenta, las centrales telefónicas de las rutas más ocupadas ya estaban muy saturadas, por lo que necesitaron mayor ancho de

[1] Ver Anexos (Puertas Logicas)

banda que el de los regulares pares de cables de cobre podían aguantar. Por ello las compañías telefónicas empezaron a usar cables coaxiales.

En los sesenta, con la emergencia de la industria de televisión por cable, que es un fuerte consumidor de ancho de banda, además de los cada vez mayores requerimientos de capacidad de conducción de las empresas telefónicas, en los años sesenta el consumo de ancho de banda aumentó considerablemente. Se recurrió al cable coaxial y a la tecnología digital que solventaron el requisito de mayor eficiencia en el uso del ancho de banda. Sin embargo, simultáneamente se empezaron a buscar otros conductores que usaran alguna forma de comunicación óptica, esto es, usando luz en vez de microondas.

Los primeros estudios sobre las fibras ópticas para aplicaciones de transmisión se llevaron a cabo a mediados de los sesenta. En el laboratorio de la Standard Telecommunications de ITT en Inglaterra, C.K. Kao y G.A. Hockham postularon que las ondas de luz se podían guiar por vidrio, o sea, fibra óptica, donde la luz que entra por un extremo de un hilo se refleja repetidamente en las paredes de la fibra con un ángulo crítico bajo y sale por el otro extremo con el mismo ángulo, igual que si pasara por una tubería. En 1970 los científicos de Corning Glass Works en Nueva York convirtieron la idea en realidad. Los ensayos de campo se empezaron en 1975 y en 1978 se habían instalado 1000 kilómetros de fibra óptica por el mundo.

Canadá fue uno de los pioneros en la instalación de redes de fibra óptica. En 1966, Bell Northern Research instaló un sistema de comunicaciones ópticas totalmente operativas en el Ministerio de la Defensa Nacional. También en 1981 se tendió una red rural, conocida como Proyecto Elie, en dos comunidades de la provincia de Manitoba donde no había ningún servicio de telecomunicación; y con la fibra óptica se llevaron a 150 hogares, servicios telefónicos, televisión por cable, radio en FM y videotexto.

En 1983 en Estados Unidos ATyT terminó el primer circuito de fibra óptica de larga distancia entre Washington y Boston. En ese mismo año se instalaron 15 rutas de larga distancia en Inglaterra, Escocia y Gales.[59] Para 1980 había instalados 6 mil kilómetros de fibra óptica en el mundo que aumentaron a aproximadamente 160 mil hacia 1989.

¿Qué son las Fibras ópticas?

Las fibras ópticas son hilos finos de vidrio generalmente o plástico, guías de luz (conducen la luz por su interior). Generalmente esta luz es de tipo infrarrojo y no es visible al ojo humano. La modulación de esta luz permite transmitir información tal como lo hacen los medios eléctricos con un grosor del tamaño de un cabello humano, poseen capacidad de transmisión a grandes distancias con poca pérdida de intensidad en la señal y transportan señales impresas en un haz de luz dirigida, en vez de utilizar señales eléctricas por cables metálicos. Este es el medio de transmisión de datos inmune a las interferencias por excelencia, con seguridad debido a que por su interior dejan de moverse impulsos eléctricos, proclives a los ruidos del entorno que alteren la información. Al conducir luz por su interior, la fibra óptica no es propensa a ningún tipo de interferencia electromagnética o electrostática.

1.3.41 estructura de la fibra óptica

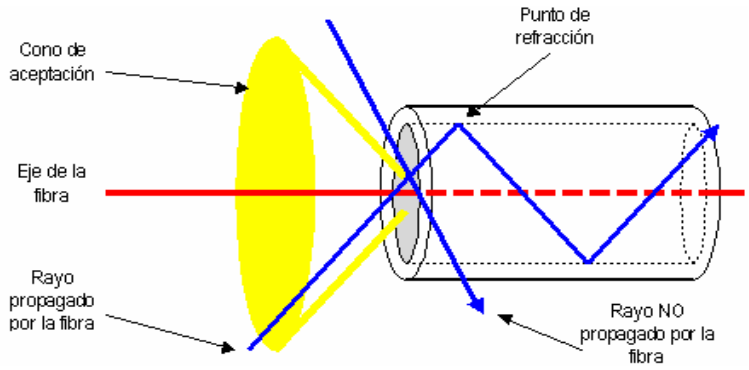
La estructura de la fibra óptica es relativamente sencilla, aunque la mayor complejidad radica en su fabricación. La fibra óptica está compuesta por dos capas, una de denominada Núcleo (Core) y la otra denominada Recubrimiento (Clad). La relación de diámetros es de aproximadamente 1 de recubrimiento por 3 de núcleo, como se ilustra en la figura 1. El extra delgado hilo de vidrio está cubierto por una capa plástica que le brinda la protección necesaria, aunque normalmente un gran conjunto de fibras se unen entre sí para obtener mayor seguridad como veremos un poco más adelante.

Para manipular la fibra óptica, esta se incorpora dentro de una estructura mayor que asegura su funcionalidad y conservación. Este grupo de varias fibras ópticas es conocido con el nombre de cable óptico. Un elemento central de tracción con un recubrimiento de polietileno es empleado para evitar tensiones y tracciones que puedan romper una o varias de las fibras contenidas en su interior. Las fibras están recubiertas por una cinta helicoidalmente dispuesta, con una vaina exterior que recubre todo el conjunto. Se pueden apreciar dos tipos de cables ópticos en la figura 1.

Como se propaga la información (luz) en la fibra óptica

La fibra óptica está compuesta por dos capas de vidrio, cada una con distinto índice de refracción. El índice de refracción del núcleo es mayor que el del revestimiento, razón por la cual, y debido a la diferencia de índices la luz introducida al interior de la fibra se mantiene y propaga a través del núcleo. Se produce por ende el efecto denominado de Refracción Total, tal como se ilustra en la figura 2. Los rayos de luz pueden entrar a la fibra óptica si el rayo se halla contenido dentro de un cierto ángulo denominado CONO DE ACEPTACIÓN. Un rayo de luz puede perfectamente no ser transportado por la fibra óptica si no cumple con el requisito del cono de aceptación. El cono de aceptación está directamente asociado a los materiales con los cuales la fibra óptica ha sido construida. La figura 3 ilustra todo lo dicho. Respecto a atenuaciones producidas dentro de otros medios de transmisión, la fibra óptica presenta niveles de atenuación realmente bajos que permiten transmitir luz por varios kilómetros sin necesidad de reconstruir la señal (regenerar).

Figura 5 Fibra Óptica



LONGITUD DE ONDA.- Todo rayo de luz se halla dentro de un espectro posible. El espectro incluye en la parte más izquierda, los rayos de luz de menor longitud de onda, pero que poseen más energía, denominados ultravioletas. En el otro extremo, se halla las luces de mayores longitudes de onda, pero que poseen menor energía, a las que se denomina infrarrojas. Un intervalo relativamente pequeño de todo este espectro, que se halla entre los colores violeta y rojo, es el que el ojo humano puede apreciar. Son precisamente las luces que se hallan dentro del espectro correspondiente a los infrarrojos los que se emplean para transmitir información por el interior de las fibras ópticas.

1.3.42 La dispersión de la luz, un problema en las fibras ópticas

Este es uno de los fenómenos típicos perjudiciales que se producen Dentro de la transmisión por fibra óptica. Por el efecto de la dispersión, todo rayo que viaja por una fibra se va "ensanchando" a medida que avanza por la misma. Los cálculos para la introducción de repetidores regenerativos deben contemplar este fenómeno. Es cierto que la fibra más que ningún otro medio de transmisión es ideal para transmitir a largas distancias, sin embargo el fenómeno de dispersión de la luz se produce y debe ser tenido muy en cuenta.

Dentro del tema de los receptores existe una cantidad de términos muy interesantes.

A continuación los mismos.

Foton / Electron.- Dentro de la transmisión eléctrica, la unidad se denomina electrón. Dentro del sistema óptico, la unidad óptica se denomina fotón.

Responsabiidad y deficiencia cuantica: Es el número de electrones generados por la incidencia de un cierto número de fotones recibidos. La eficiencia de un fotodetector APD es mucho mayor que la correspondiente a un PIN o PIN-FET. CORRIENTE DE PÉRDIDA.- Es la corriente que circula a través de la juntura sin la presencia de luz incidente. Todo receptor tiene algún voltaje que lo mantiene operativo, la corriente de pérdida hace referencia a la misma.

1.3.43 Ruido Cuántico

El ruido cuántico es el producto de la conversión del sistema fotónico al sistema eléctrico. Está compuesto por ligeras variaciones producto de este cambio.

Tiempo de crecimiento: Es el tiempo que un receptor tarda en predisponerse para la captura de información. El APD tiene un tiempo muy breve, y se convierte en el dispositivo ideal para capturar información a alta velocidad.

Los elementos de instalaciones para fibra óptica son los siguientes.

Repetidores: Aunque en baja escala, la señal que se transmite por la fibra óptica es atenuada. A fin de que la señal no se convierta en imperceptible, se deben instalar repetidores en sistemas que cubran grandes distancias.

Empalmes: Son interconexiones permanentes entre fibras. En este caso, los núcleos de las fibras que se unan deben estar perfectamente alineados a fin de que no se produzca ninguna pérdida. Dentro de los empalmes, existen dos formas de los mismos. Los primeros son los EMPALMES POR FUSIÓN, en la cual las dos fibras ópticas son calentadas hasta obtener el punto de fusión, y ambas quedan unidas. Este método siempre tiene una ligera pérdida de 0.2dB.

El segundo tipo es el EMPALME MECÁNICO, en el cual, por elementos de sujeción mecánicos, las puntas adecuadamente cortadas de las fibras se unen, permitiendo el pasaje de la luz de una fibra a otras. La pérdida de información en este segundo caso, es ligeramente mayor al primer caso, de 0.5dB.

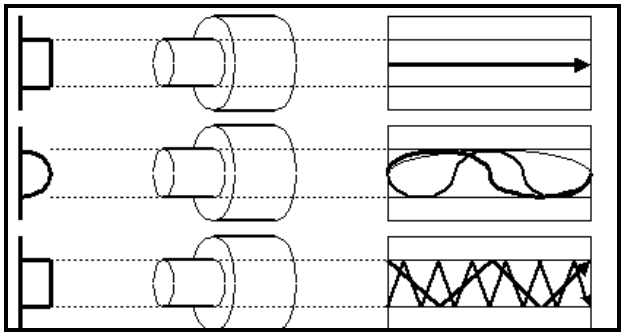
Conectores: Son conexiones temporales de fibras ópticas. Este sistema debe tener una precisión grande para evitar la atenuación de la luz. Suelen emplear los denominados Lentes Colimadores, produciendo pérdidas de 1dB.

Acopladores: Existen dispositivos que permiten distribuir la luz proveniente de

una fibra, hacia otras. Son dos tipos de acopladores los que existen: en T y en estrella. Los acopladores en T permiten distribuir la luz proveniente de una fibra, hacia dos salidas, por lo general una entra a una computadora, y la otra prosigue hacia las siguientes. Los acopladores en estrella permiten distribuir una sola entrada de información hacia muchas salidas. Estos últimos pueden ser de 3 a 40 puertas. Todo acoplador tiene una pérdida aproximada de 5dB.

1.3.44 Tipos de Fibras ópticas

Figura 6 Tipos e Fibra



Las fibras ópticas se clasifican de acuerdo al modo de propagación que dentro de ellas describen los rayos de luz emitidos. En esta clasificación existen tres tipos. Los tipos de dispersión de cada uno de los modos pueden ser apreciados en la figura anterior.

Monomodo: En este tipo de fibra, los rayos de luz transmitidos por la fibra viajan linealmente. Este tipo de fibra se puede considera como el modelo más sencillo de fabricar, y sus aplicaciones son concretas.

Multimodo - Graded Index: Este tipo de fibra son más costosas, y tienen una capacidad realmente amplia. La tecnología de fabricación de las mismas es realmente importante. Sus costos son elevados ya que el índice de refracción del núcleo varía de más alto, hacia más bajo en el recubrimiento. Este hecho produce un efecto espiral en todo rayo introducido en la fibra óptica, ya que todo rayo describe una forma helicoidal a medida que va avanzando por la fibra

Multimodo - Step Index: Este tipo de fibra, se denomina de multimodo índice escalonado. La producción de las mismas resulta adecuado en cuanto a tecnología y precio se refiere. No tiene una capacidad tan grande, pero la

calidad final es alta. El índice de refracción del núcleo es uniforme para todo el mismo, en realidad describe la forma general de la fibra óptica.

1.4 Conceptos Básicos de Mecánica Cuántica

1.4.1 La Teoría Cuantica

Según la teoría clásica del electromagnetismo la energía de un cuerpo caliente sería infinita!!!

Esto es imposible en el mundo real, y para resolver este problema el físico Max Plank inventó la mecánica cuántica.

1.4.2 ¿En Que Consiste la Mecánica Cuantica?

Los sistemas atómicos y las partículas elementales no se pueden describir con las teorías que usamos para estudiar los cuerpos macroscópicos (como las rocas, los carros, las casas, etc). Esto de debe a un hecho fundamental respecto al comportamiento de las partículas y los átomos que consiste en la imposibilidad de medir todas sus propiedades simultáneamente de una manera exacta. Es decir en el mundo de los átomos siempre existe una INCERTIDUMBRE que no puede ser superada. La mecánica cuántica explica este comportamiento.

1.4.3 ¿Entonces que Dice la Mecanica Cuantica?

El tamaño de un núcleo atómico es del orden de 10-13 centímetros. ¿Podemos imaginar ésto? Muy difícilmente. Mucho más difícil aún sería imaginar como interactúan dos núcleos atómicos, o cómo interactúa el núcleo con los electrones en el átomo. Por eso lo que dice la mecánica cuántica muchas veces nos parece que no es 'lógico'. Veamos que propone la mecánica cuántica:

El intercambio de energía entre átomos y partículas solo puede ocurrir en paquetes de energía de cantidad discreta (Fuerzas e Interacciones)

Las ondas de luz, en algunas circunstancias se pueden comportar como si fueran partículas (fotones).

Las partículas elementales, en algunas circunstancias se pueden comportar como si fueran ondas.

Es imposible conocer la posición exacta y la velocidad exacta de una partícula al mismo tiempo. Este es el famoso Principio de Incertidumbre de Heisemberg

2 COMPUTACIÓN CUÁNTICA

El principal objeto a vencer es que la física o mecánica normal cualquier sistema puede estar en solo un estado, mientras que en la computación cuántica esto ya no es una limitante para los objetos, puede estar en mas de un estado a la vez; Por ejemplo en la física clásica podemos decir que la F= ma (Fuerza = masa * aceleración) pero para la física cuántica esto presenta una indefinición tanta con el transcurrir del tiempo que no podemos asegura esto en una partícula, no puedo ver el estado real de la partícula como del sistema en si.

Esto se tiene que determinar por medio de la probabilidad de que una partícula este en un estado o en otro. El modelo de computación cuántica habla de la superoposición, o sea tener más de una posición en un momento dado, pero como hago para saber la posible posición, esto se basa en la probabilidad.

La superposición de estados es como se explica la composición de colores, por ejemplo, el color anaranjado esta compuesto por un porcentaje de parte de color rojo y otra de color amarillo, y esto esta en la superposición esta determinado por unos factores numéricos, dándoles a estos factores un valor probabilística de que el sistema este en un estado u otro.

Otro aspecto importante y muy relevante dentro de lo que es la computación cuantica es, el hecho de que estamos habando de que necesitaríamos para poder hacer muchas operaciones en paralelo la misma cantidad de CPU’s por cada una de las operaciones que necesitemos hacer en paralelo.

Por ejemplo si tengo 1 operación, para hacerla en paralelo, necesito un CPU pero si ya son 2 necesito 2 CPU's y así sucesivamente por lo cual la cantidad de CPU's crece exponencialmente para hacer muchas operaciones en paralelo, esto de por si ya nos da una limitante, la cual es el espacio físico para la cantidad de CPU's que necesitemos según la cantidad de operaciones en paralelo que queramos hacer, es aquí donde la computación cuántica nos puede ayudar ofreciéndonos la posibilidad de hacer muchas operaciones en paralelo con una sola pieza de Hardware.

Suponga un calculo sencillo de la fuerza de un objeto F= ma si queremos calcular la fuerza de una masa de 10 kg y una aceleración de 10 km/h seria igual a 100 NWTS, ahora los mismo solo que para 9 kg y 9 km/h seria 81NWTS este calculo sencillo no lleva el doble de tiempo por cada una de las variables; Imagínese con mas variable y mas datos a usar, esto tomara mas y mas tiempo según la cantidad de datos y de variables.

Cuando se vio el concepto, de que al mismo tiempo se pueden hacer dos o mas cálculos con una computadora cuantica, basándonos en el concepto de superposición de la cuantica, del cual hablaremos adelante, esto hizo que los científicos pensaran que es imposible o como lo expresaron algunos que era muy bueno poder hacer muchos calculo en el mismo lapso de tiempo como para que fuera cierto.

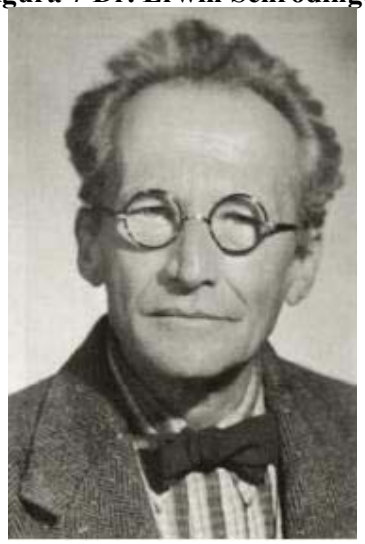
Esto ofrecía poder hacer muchas operaciones en paralelo sin la necesidad de mucho hardware solo para iniciar, por supuesto que hay un precio que pagar por esto, que es el no poder leer todas las respuestas intermedias e incompletas. Lo mejor que podemos esperar es que haga es una calculo rápido y preciso que dependen de muchos caminos que están juntos. Por eso no podemos ver las repuestas de algunos resultados intermedios individualmente, si no solo la respuesta del problema final que es lo que realmente nos interesa.

Esta parte es muy importante pues las personas pregunta por que no se usa la computación cuantica para medir el clima, o para modelos aerodinamicos, los cuales usan muchos cálculos paralelos para esto; Esto un día se podrá hacer, pero por el momento se esta creando el modelos, luego de que se perfecciones, ya saldrán programas que incluyan esto que es cálculos de temperatura, de humedad billones de diferentes puntos escenarios, y en espacios en 3-D. Pues los programas podrán tener la flexibilidad completa y la formulas matemáticas para poder hacer y predecir todo la parte de paralelismos de la que por el momento no contamos.

2.1 El significado de la Superoposición:

Para poder explicar este término de superposición debemos de hacer un llamado al experimento de doctor Schrödinger, el cual se llama el experimento del gato.

Figura 7 Dr. Erwin Schrodinger



El doctor Erwin Schrödinger

Schrödinger sugirió realizar el siguiente montaje: se mete un gato dentro de una caja —hasta aquí todo más o menos normal— que contiene una ampolla de vidrio en la que se ha encerrado un potente veneno volátil.

Hay, además, un artefacto capaz de romper el cristal, que consiste en un martillo sujeto encima de la ampolla. El martillo puede ser liberado eléctricamente y está conectado a un mecanismo detector de partículas alfa. Si llega al detector una partícula alfa el martillo cae, rompe la ampolla y el gato muere. Si por el contrario no llega ninguna partícula no ocurrirá nada y el gato continúa vivo.

El experimento se completa colocando un átomo radiactivo en el detector. Este átomo es inestable, por lo que existe un 50% de probabilidades de que, en una hora, emita una partícula alfa. Es evidente que al cabo de una hora habrá ocurrido uno de los dos posibles desenlaces: o el átomo ha emitido una partícula alfa o no la ha emitido. La probabilidad de que ocurra una cosa o la otra es idéntica.

El resultado de toda esta interacción es que el gato del interior de la caja está vivo o está muerto. Pero no podemos saberlo si no la abrimos para comprobarlo.

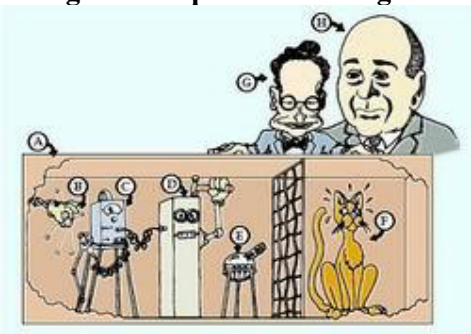
Si se describe lo que ocurre en el interior de la caja aplicando las leyes de la mecánica cuántica, se llega a una conclusión muy extraña. El gato estará descrito por una función de onda extremadamente compleja, resultado de la superposición de dos estados combinados al cincuenta por ciento: "gato vivo" y "gato muerto". Es decir, aplicando el formalismo cuántico, mientras no se lo observa el gato está a la vez vivo y muerto; se trata de dos estados indistinguibles.

La única forma de averiguar qué ha ocurrido con el gato es realizar una medición: abrir la caja y mirar dentro. En unos casos nos encontraremos al gato vivo y en otros casos estará muerto. Pero, ¿qué ha ocurrido? Según la mecánica cuántica, al realizar la medida el observador interactúa con el sistema y lo altera, rompe la superposición de estados y el sistema se decanta por uno de sus dos estados posibles.

El sentido común nos indica que el gato no puede estar vivo y muerto a la vez. Pero la mecánica cuántica dice que mientras nadie mire en el interior de la caja el gato se encuentra en una superposición de los dos estados: vivo y muerto.

Lo dramático del planteo de Schrödinger ya cumplió su efecto y ahora se puede reemplazar el mecanismo por uno que incline o no una botella de leche —por dar un ejemplo que se maneja en la didáctica de hoy— y nos dé, en lugar de "gato muerto" y "gato vivo" una paradoja más suave —pero obviamente muchísimo menos efectiva—: "gato alimentado" y "gato hambriento".

Figura 8 Experimento del gato



2.2 La novedad macroscópica

El experimento del gato es físicamente posible, y quizás algún día se pueda realizar, pero es muy dificultoso de llevar a la práctica, porque se debe aislar un átomo y se debe estar seguro de que aún no ha emitido su partícula alfa. En estos días un equipo de físicos ha publicado la receta para poner un objeto grande —no del tamaño de un gato, por cierto, sino del de una bacteria, es decir que se puede ver en un microscopio— en un estado cuántico así. Según proponen en su nuevo experimento, un espejo minúsculo puede estar en dos lugares a la vez.

Aunque para el sentido común no parece posible, de hecho esto sucede todo el tiempo, claro que a nivel cuántico. Los científicos se han resignado a que las entidades del tamaño de átomos son capaces de estas hazañas, pero por lo general se asume que a escalas mayores interviene un fenómeno llamado decoherencia, que deja fuera las rarezas cuánticas, lo que pone a los objetos cotidianos en una ubicación única y definida.

2.3 ¿Decoherencia?

Un sistema cuántico clásico debe satisfacer condiciones. Una de ellas es que, dado que en general todo estado de un sistema cuántico corresponde a una superposición (superposición de estados electrónicos, "gato vivo" y "gato muerto", etc.), es requisito que exista algún mecanismo por el cual esta superposición sea inestable y decaiga a un estado bien definido: el de "gato vivo" o el de "gato muerto".

Este proceso se conoce con el nombre de decoherencia y se basa en el hecho de que los sistemas físicos no están aislados sino que interactúan con muchos otros, y esta interacción es la responsable de que a nivel clásico desaparezcan los estados de superposición. Este proceso de pérdida de coherencia permite que lo que en principio es un sistema cuántico se pueda describir en términos de variables clásicas.

Para explicar en forma gráfica el origen del nombre decoherencia conviene primero entender el concepto de coherencia. Esto se puede hacer con un ejemplo sencillo de ondas mecánicas.

Si tiramos una piedra en un estanque de agua, se genera una onda circular que se expande. Esta onda tiene una característica: la distancia entre el máximo y el mínimo de la onda no cambia a lo largo del tiempo. La fase de la onda no cambia, lo que significa que la onda es coherente.

Si tiramos dos piedras en el estanque, muy cerca, se generan ondas circulares a partir de cada una de ellas. Al chocar una contra la otra se observa que, en determinados lugares, las ondas se suman, aumentando la amplitud de las oscilaciones, mientras que en otros las ondas se suman destructivamente (se restan o anulan), haciendo desaparecer las oscilaciones. Para que este fenómeno de interferencia se manifieste es necesario que las ondas sean coherentes, de lo contrario no se produce ningún patrón de máximos y mínimos.

Los estados cuánticos presentan una relación definida de fase (coherencia) entre las componentes de la superposición. Si uno logra, mediante algún mecanismo ingenioso, hacer interferir cada componente, se obtendrán los patrones que mencionamos recién.

Pero la interacción entre un sistema representado por una superposición con otros sistemas hace que la constancia de la relación de fase entre las componentes decaiga en el tiempo, produciéndose decoherencia, y la consecuente desaparición del patrón de interferencia que está asociado a la superposición.

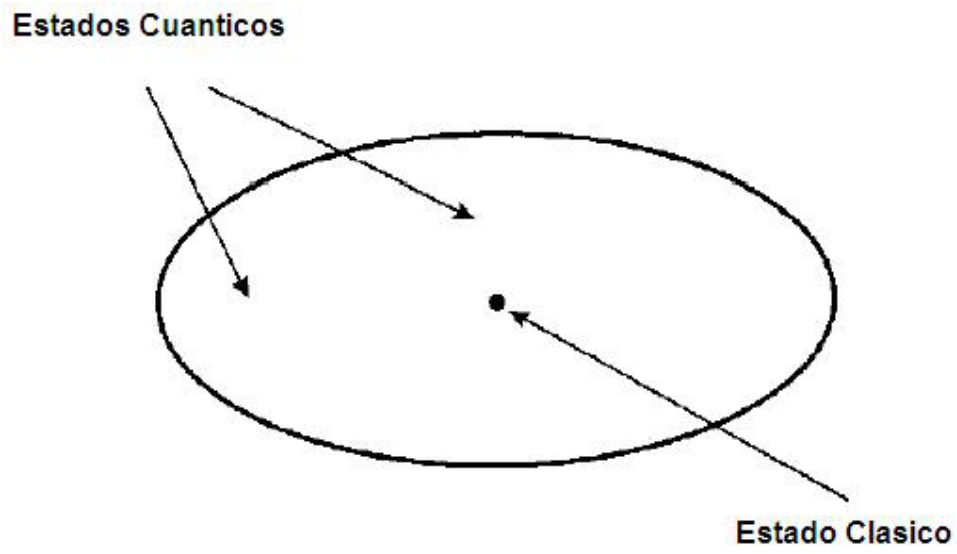
2.4 Espacio de Hilbert

Esto se lo debemos a David Hilera, matemático Alemán, el cual nos dice; Este no es un espacio de la forma convencional, si no mas bien es un espacio de estados convencionales, Un mapa de estados convencionales es un circulo que define o describe todos los posibles estado y sus movimientos, incluyendo la trayectoria de rotación de una coordenada a otra si es que da algún giro.

El espacio de Hilbert no es mas que esto, solo que tomando en cuenta todos los diferentes vectores siguiendo todas las posibles direcciones, esto da mucha mas libertad y esta libertad nos da muchas dividendos, pues esto quiere decir que podemos hacer muchos cálculos mas rápido por que estamos acensando a un espacio mucho muy largo sino infinito.

El espacio de Hilbert expande la matemática abstracta en forma inimaginable, pues nos da como resultado la suma de todos los posibles estados de un estado clásico. Por ejemplo si el estado clásico es 0 y 1 el espacio de Hilbert es la suma de ambos estados o sea es estado de 0 y el estado de 1.

Figura 9 La Grandeza del Espacio de Hilbert

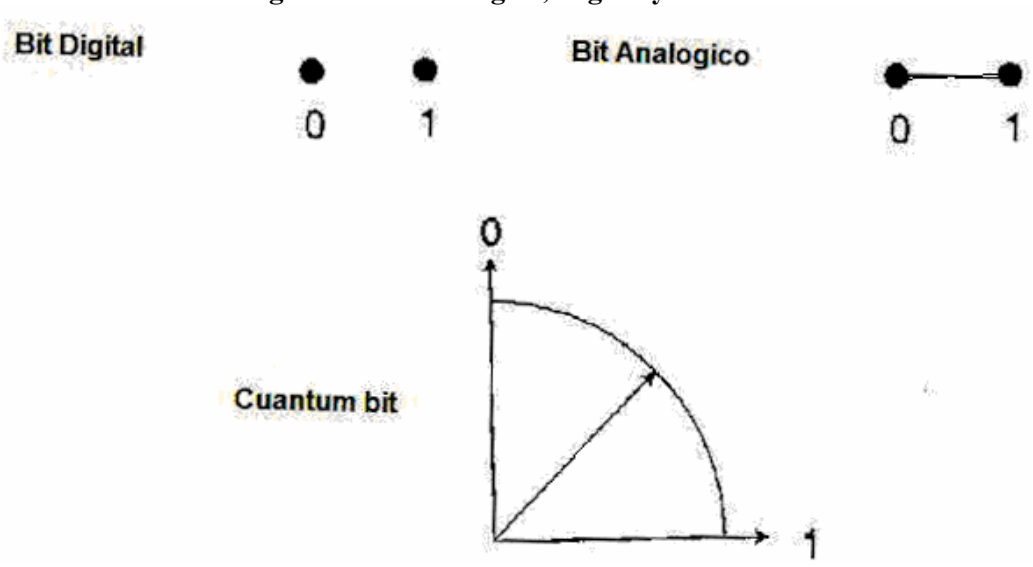


El termino superposición viene del estudio de fenómeno de Ola. Cuando una ola de agua, por ejemplo, llega en diferentes direcciones, el efecto combinado se puede calcular por la suma de las diferentes olas, en otras palabras, superponiendo una ola sobre la otra. La superposición de un estado del electrón que viene por que de acuerdo a mecanismos cuanticos todas las partículas Duch es un electrón con aspecto de olas. Esto es, en teoría, un infinito numero de diferentes superposiciones, nosotros podemos hacer, porque cuando la luz esta brillando por diferente largo de tiempo, el electrón toma en un rango de diferentes estados de superposiciones.

Usado de esta forma el átomo solo puede guarda una unidad de información quántica, sabemos que un quantum bit o qbit. Un qbit por consiguiente difiere de un bit analógico convencional en que este puede guardar valores intermedios entre el 0 y 1. Superficialmente un qbit puede parecer muy similar a un bit análogo por la información que es acarreada or, una señal eléctrica que puede tomar cualquier valor de voltaje entre 0 y 1 (Ver figura de abajo). Pero hay una diferenta fundamental entre el qbit y una bit análogo; como siempre una medida es hecha por un qbit , la respuesta solo puede ser una 0 o 1, no algún valor intermedio como podemos esperar de una señal analógica. Esta diferencia, como veremos, trae muchas consecuencias diferentes.

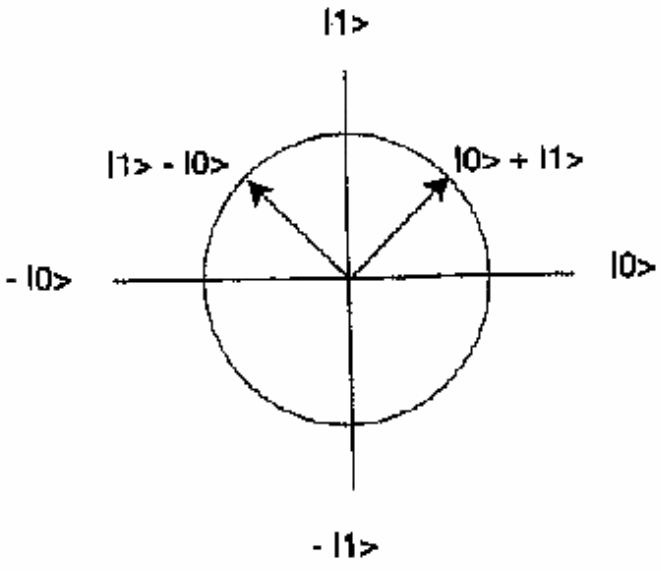
Bit's clásicos digitales son agrupados dentro de la computadora para representar números largos. Un registro de 2 bits puede representar algún numero entre 0 y 3 por que, juntos, los 2 bits pueden tomar los valores 00,01,10 y 11, tomando la representación de base 2 para números que sabemos mejor, 0,1,2,3. Dos qbits pueden representar similarmente cada uno de estos valores, como bit ordinarios. Sin embargo, dos qbit pueden ponerse en estado de superposición uno o todos estos estados. De ese modo un registro quantico de 2 qbits puede representar simultáneamente 0,1,2 o 3. Si nosotros consideramos un registro de 8 qbits, podemos obtener una representar una superposición de $2^{8} = 256$ números, un registro de 1,000 qbits puede representar 2^{1000} (Aproximadamente 10^{300} números) simultáneamente. En contraste, un registro clásico de 1000 bits.

Figura 10 Bit analogico, Digital y Cuántico



Información digital viene en representación de bits por 0s y 1s. Una bit análogo toma algún valor entre 0 y 1. Un qbit puede existir en superposición de 0 y 1, que podemos representar por un puntero vector en una dirección intermedia entre estas representaciones 0 y 1.

Figura 11 Representación vectorial de los estados de bit cuántico



2.5 Entropía de la Información

Entropía de Shannon.

Sea X una *variable aleatoria,* que toma el valor x con probabilidad p(x). Definimos el *contenido de información*, o *entropía* de X como:

$$S(\{p(x)\}) = -\sum_x P(x)\log_2 p(x) \qquad (1)$$

Ahora queda interpretar esta definición: Que utilicemos base 2 para el logaritmo es simple cuestión de convenio. La entropía es siempre positiva, dado que p(x) está normalizada a la unidad, y por tanto el logaritmo resulta negativo o cero. S es una función de la *distribución de probabilidades* de los valores de X. Es normal que esto sea así, dado que mayor información esperaremos obtener de la cantidad X si los valores que puede tomar son equiprobables que si alguno de ellos es casi seguro. En lo sucesivo indicaré S({p(x)}) como S(X), no perdiendo de vista lo que en realidad significa. Estamos acostumbrados a hablar de entropía en el contexto de la física estadística, pero definida de este modo adquiere significado en cualquier disciplina donde el grado de conocimiento que tengamos sobre un sistema sea importante, como en biología o economía.

Veamos algún ejemplo sobre cómo funciona esta expresión:

1. Supongamos que sabemos de antemano que X tomará el valor 2, es decir, la distribución de probabilidad es una delta:

$$P(x) = \delta \qquad (2)$$

o bien, p(x)=0 para $x \neq 2$; p(2)=1. Todos los valores posibles de x son recorridos por la sumatoria, pero sólo cuando x=2 tendremos un término no nulo:

$$-\sum_x P(x)\log_2 p(x) = P(2)\log_2 p(2) = -\log_2(1) = 0$$

En otras palabras, no aprendemos nada, como dije antes. X no contiene información.

2. Consideremos la situación en la que el valor de X viene dado al tirar un dado. Los valores posibles para X son los enteros, del uno al seis {1,2,3,4,5,6}, todos ellos en principio con la misma probabilidad, $\frac{1}{6}$. Si sustituimos las cantidades en la expresión (1):

$$-\sum_x P(x)\log_2 p(x) = -\sum_1^6 [1/6\log_2(1/6) = -\log_2(1/6) \approx 2.58$$

Cuando X puede tomar N valores diferentes, el valor de la entropía se maximiza cuando todos tienen igual probabilidad, p(x)= N^{-1}. Sobre esto ya apunté algo antes. Ganaremos más información al conocer el valor que toma X cuanto menos sepamos en principio sobre cuál puede ser. El que los posibles valores de X sean equiprobables es claro que hace máxima nuestra incertidumbre. La máxima cantidad de información que puede almacenarse en una varible que puede tomar N valores diferentes corresponde a todos con probabilidad $\frac{1}{N}$, es decir:

$$S\max(X) = -\log_2(1/N) = -\log_2(n)$$

$$X \in \{x_i\}_1^n = 1$$

¿Y cuánto vale la unidad de información?

Si partimos del análisis de una variable que puede tomar sólo dos valores con igual probabilidad, al aplicar la ecuación 1 encontramos S(X)=1. Esto va asociado al hecho de haber elegido base 2 en la definición. Otra escala habría llevado a otras medidas, claro, y a una unidad de entropía con un valor diferente, pero somos libres de escoger, al igual que hacemos con cualquier otra magnitud.

Cuando una variable puede tomar sólo dos valores, es claro que la probabilidad de que tome uno de ellos depende de la de que tome el otro. Si X puede valer sólo 1 o 0, entonces p(x=0)=1-p(x=1), pues el sistema no puede escoger más alternativas. Todo el contenido informativo de X depende entonces de una única probabilidad. Sustituyendo en la ecuación 2 los parámetros correspondientes a un sistema de este tipo:

$$H(p) = -p\log p - (1-p)\log_2(1-p)$$

Obtenemos la entropía de un sistema de dos estados o, en adelante, simplemente *función entropía*. La función entropía de este modo definida toma valores entre 0 y 1.

2.5.1 Entropía condicional e información mutua.

La entropía condicional se define a partir de la probabilidad condicionada. Representamos la probabilidad de que dado un valor X=x para un parámetro, tengamos Y=y, como p(x|y). A partir de él, la entropía condicional S(x|y) se define como:

$$S(x/y) = \sum\ p(x) \sum_y\ p(y/x) \log p(y/x) = -\sum_x\ \sum_y\ p(x,y) \log_2 (y/x)$$

La segunda de las igualdades se obtiene de

$$p(x,y) = p(x)p(x/y) \quad (2)$$

que es la probabilidad de que X=x al mismo tiempo que Y=y.

Podemos interpretar la definición observando que S(x|y) da una idea de cuanta información permanecería oculta en Y si estuviésemos interesados en el valor de X. Conviene observar que Y contendrá menos información en general, nunca más, cuanto más sepamos sobre X, y que ambas variables no tienen por que determinar el valor de la otra en igual medida:

$$S(Y/X) \leq S(Y)$$

$$S(Y/X) \neq S(Y)$$

La primera de estas expresiones se convierte en una igualdad cuando el valor de X no determina de ningun modo el valor de Y. Sobre la segunda expresión, podemos imaginar, por ejemplo, una relación condicional, pero no biunívoca. De este modo podríamos utilizar:

``*Si X toma valor 2, entonces Y tomará valor cero''*

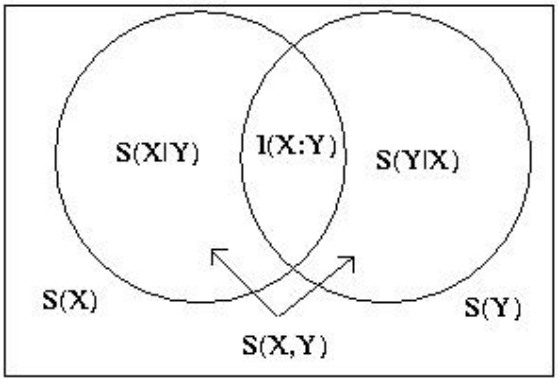
En esta situación, saber que X=2 determina completamente el valor de Y, mientras que conocer el valor de Y no nos dice nada sobre el de X.

A partir de la entropía condicional podemos definir la *información mutua* como :

$$I(X;Y) = \sum_x \sum_y p(y/x) \log_2 \frac{p(x,y)}{p(x)p(y)} = s(X) - S(X \mid Y) \quad (3)$$

Esta cantidad da idea de cuanta información contiene cada variable sobre la otra. Si se trata de variables independientes entonces p(x,y)=p(x)p(y), y la información mutua es *ninguna*. La siguiente figura procede de la ecuación de inicio de este apartado de entropía condicional, como casi todo el apartado, pero he creído conveniente incorporarla porque ilustra muy bien estas ideas

Figura 6 Variables con información mutua



Comprobaré ahora que el contenido informativo de la pareja (X,Y), esto es, la información que obtendríamos al averiguar ambos valores sin conocer inicialmente ninguno, obedece a:

$$S(Y/X) = S(X) + S(Y) - i(X;Y)$$

Esto es, la suma de la información asociada a ambas variables menos la que comparten, para no duplicarla. Para hacerlo recurriré a la definición de entropía, ecuación 1:

$$S(Z) = -\sum_x p(z) \log_2 p(z)$$

Donde Z es el hecho compuesto (X,Y). De este modo, Z=z significará que (X,Y)=(x,y). Ahora el problema se reduce a sustituir la probabilidad p(z)

en la expresión anterior. Se trata de la probabilidad de que simultáneamente X e Y tomen unos valores previstos. Esto podemos hacerlo utilizando Ecuación 2:

$$S(Z) = -\sum_z \; p(x,y)\log_2 p(x,y) = -\sum_z \; \sum_y \; [p(x)p(y \mid x)\log_2\{[p(x)p(y \mid x)]\}$$

desarrollando:

$$S(X,Y) = -\sum_x \; p(x)\sum_y \; p(y \mid x) = [\log_2 p(x) + \log_2 p(y \mid x)]$$

$$S(X,Y) = -\sum_x \; p(x)\sum_y \; p(y \mid x)\log_2 p(x) - \sum_x \; p(x)\sum_y \; p(y \mid x)\log_2 p(y \mid x)$$

Utilizando la definición de información mutua Ecuación 3 puedo poner la expresión anterior como:

$$S(X,Y) = -\sum_x \; \sum_y \; p(x)p(y \mid x)\log_2 p(x) - \sum_x \; \sum_y \; p(x)p(y \mid x)\log_2 p(y \mid x) +$$

$$+\sum_x \; \sum_y \; p(x)p(y \mid x)\log_2 p(x) - \sum_x \; \sum_y \; p(x)p(y \mid x)\log p(y)$$

Donde he sumado y restado un término al final. Agrupando convenientemente:

$$S(X,Y) = -\sum_{x,\,y} p(x)p(y \mid x)\log_2 p(x) - \sum_{x,\,y} p(x)p(x \mid y)\log_2 p(y) - \sum_{x,\,y} p(x,y)\log\frac{p(x \mid y)}{p(y)}$$

Multiplicando y dividiendo por p(x) los argumentos del logaritmo:

$$S(X,Y) = -\sum_{x,\,y} p(x)p(y \mid x)\log_2 p(x) - \sum_{x,\,y} p(x)p(x \mid y)\log_2 p(y) -$$

$$-\sum_{x,\,y} p(x)p(y \mid x)\log\frac{p(x)p(x \mid y)}{p(x)p(y)}$$

Que no es otra cosa que:

$$S(X;Y)=S(X)+S(Y)-I(X;Y)$$

Basta con interpretar los términos para comprobarlo, teniendo en cuenta que la probabilidad de obtener X=x o Y=y está condicionada por el valor de la otra variable.

Por otra parte, si bien la información puede perderse, esta no puede surgir de ninguna parte. Esto lo expresamos por medio de la *desigualdad del procesamiento de datos*:

$$(X \rightarrow Y \rightarrow Z) \rightarrow I(X;Z) \leq I(X;Y)$$

Esto es, si X conduce a Y, e Y conduce a Z (hablamos de una cadena markoviana [2]), entonces la información que comparte X con Z en ningún caso podrá ser mayor que la que comparte con Y. En un proceso de este estilo Z depende directamente de Y, pero no de X:

$$P(x,y,z)=p(x)p(y|x)p(z|y)$$

Una forma de expresar lo que ocurre es, al tratar a Y como un procesador de la información, decir que no puede transmitir a Z más información que la que recibe de X.

2.5.2 Entropía de Von Neumann.

Antes de nada preocupémonos de si el qubit es una buena medida de la información, como vimos que era el bit. Para ello seguiremos pasos similares a los dados en Ecuación 1.

La *entropía de Von Neumann* es una medida de la cantidad de información que obtendríamos si conociésemos el estado particular de cierto sistema cuántico, y se define como

$$S(\rho)=- T\tau\rho\log\rho$$

Donde Tr es la operación de traza, que se realiza sobre la matriz densidad, que describe un conjunto de estados de un sistema cuántico. Si comparamos con la entropía de Shannon:

$$S(X) = \sum_x p(x)\log p(x)$$

Encontramos que las definiciones son muy parecidas. Los elementos diagonales de la matriz densidad desempeñan el papel de las probabilidades

[2] Una cadena Markoviana es aquélla en la que un elemento está relacionado con el anterior y con el siguiente, pero con ningún otro más.

de que X tome cada valor. Preparemos un sistema cuántico en el estado |x>, descrito por el valor del observable X. La matriz densidad se escribe:

$$\rho = \sum_x \; p(x) \mid x >< x \mid$$

Los estados |x> no tienen por qué ser ortogonales. S(ρ) se demuestra que es un límite superior para la información mutua I(X;Y) clásica entre X y el resultado Y de la medida del sistema.

Ahora consideremos los recursos necesarios para almacenar y transmitir la información de un sistema cuántico q cuya matriz de densidad es ρ. Al igual que hicimos con la información clásica, nos gustaría reunir un número elevado de sistemas de este tipo (lo que en el otro caso llamamos secuencia típica) y utilizar un nombre que caracterice al conjunto, compactando así la información. La etiqueta será un sistema cuántico más pequeño, que valdrá como unidad de almacenaje o transmisión con todo el contenido informativo. El receptor de ese paquete reconstruirá un sistema que, cuya matriz densidad será ρ'. Para que el proceso de transmisión (o de recuperación de una información almacenada) tenga éxito la matriz densidad ρ' debe ser lo suficientemente cercana a ρ. Definimos la *fidelidad* como la cantidad que da cuenta de cuánto se parecen ambas matrices:

$$f(p,p') = \left(\mathrm{T}\tau \sqrt{\rho^{1/2}\rho'\rho}^{1/2} \right)$$

Esta cantidad puede interpretarse como la probabilidad de que q' pase un test que pretendiese determinar si el estado del sistema es ρ. En el caso de ρ y ρ' estados puros (|ϕ>< ϕ| y |ϕ'>< ϕ'|) , la fidelidad se reduce a:

$$f = |< \theta \mid \theta' >|^2$$

Que es la probabilidad de encontrar el valor propio asociado al auto-estado |ϕ> cuando el sistema se encuentra en el estado |θ'>.

Nos preocupamos naturalmente por encontrar el paquete más pequeño posible que etiquete al conjunto de estados agrupado. Análogamente al caso clásico, buscamos una fidelidad tan próxima a la unidad como sea posible:

$$f = 1 - \varepsilon; \varepsilon << 1$$

Por simplicidad, al igual que antes, nos limitamos a unidades binarias de información: sistemas de dos estados. Para un conjunto de n sistemas de 2 estados existe un vector en un espacio de Hilbert de 2^n dimensiones que especifica por completo su estado. Pero al igual que antes, esperamos que el vector de estado caiga dentro de un subespacio *típico* del espacio de Hilbert, análogamente a como los arreglos de bits tomaban valores de secuencias típicas en el caso clásico. Se demostro que la dimensión de ese sub-espacio es $2^{nS(\rho)}$, lo que por analogía con el caso anterior conduce a que sólo son necesarios nS(ρ) qubits para transmitir la información de los n sistemas. La dimensión del espacio sobre el que se representan los estados crece exponencialmente con el con número de qubits, y el qubit es una medida de información.

Importante es tener en cuenta que las operaciones de codificación y decodificación no dependen del conocimiento que tengamos sobre el estado del sistema. Esto nos salva en cierta medida del problema de la no clonación, y nos libera del hecho de tener que medir para transmitir información.

En el caso de que los estados a transmitir fuesen ortogonales entre sí el problema se reduciría al caso clásico.

Hay contrapartidas cuánticas a las otras cantidades que vimos antes: la *información coherente* desempeña el mismo papel que la información mutua, y podemos desarrollar códigos análogos al de Huffman para comunicación de información cuántica.

2.5.3 Entrelazamiento

Una propiedad responsable de la potencia de los métodos de cálculo cuánticos es el *entrelazamiento*. Una característica tan importante como esta desearíamos ser capaces de cuantificarla.

Partamos de que Alice y Bob comparten un sistema cuántico (cada uno accede acceden a una parte). Sabemos que hay entrelazamiento entre las dos partes cuando el estado del sistema no se puede representar por una superposición de productos tensoriales. Formalmente, hay entrelazamiento cuando la matriz densidad del sistema no se puede escribir como:

$$\rho^{AB} = \sum_i p_i p_i^A \otimes p_i^B$$

Donde los estados de cada subsistema no interferirían entre sí. Los superíndices A y B se refieren a los subsistemas a los que Alice y Bob tienen acceso. Tanto Alice como Bob pueden preparar cualquier estado no entrelazado por medio de transformaciones locales y de comunicación clásica: primero escogiendo el índice i, para el que deciden probabilidad p_i, después preparando los estados locales ρ_i^A y ρ_i^B. La manera en que Alice y Bob se ponen de acuerdo sobre estos estados puede tener tan poco que ver con la mecánica cuántica como tiene una simple conversación.

Veamos en cambio que ocurre si Alice y Bob pretendiesen preparar un estado entrelazado. Ahora los agentes necesitarán compartir desde el principio algún grado de entrelazamiento, cosa que pueden conseguir, si no se diese desde el principio, transmitiéndose mutuamente estados cuánticos (obsérvese que el el caso anterior sólo era necesaria comunicación clásica). Ahora sólo nos falta saber cómo hacen Alice y Bob para decidir que los estados a los que acceden están entrelazados.

Supongamos que ρ^{AB} es un estado puro (por ejemplo, $|\psi^{AB}><|\psi^{AB}$ de rango 1). En esta situación la única medida que nos

indicaría la presencia de entrelazamiento es la que se conoce como *entropía del entrelazamiento*:

$$E(\psi^{AB}) = S(\mathrm{T}\,\tau B\,\rho^{AB}) = S(\mathrm{T}\,\tau A\,\rho^{AB})$$

La entropía de entrelazamiento es la de Von Neumann de un estado mezclado cuando uno de los subsistemas se disocia. Veamos qué hemos hecho:

Una buena medida del entrelazamiento debe cumplir una serie de propiedades: dado que el entrelazamiento es un recurso cuántico, éste no podrá incrementarse vía operaciones y comunicación clásica. La mejor situación posible se da cuando dados dos estados ρ_1 y ρ_2 con entrelazamientos respectivos E_1 y E_2 ($E_{1>}$ E_2) el segundo estado es siempre identificable a partir del primero vía operaciones locales y comunicación clásica, pero esto puede ser pedir demasiado. Entonces consideramos un límite de esta situación en el que ρ_1 y ρ_2 son estados puros. Para cualquier pareja de estados puros compuestos ψ y ψ ' (conteniendo los subsistemas A y B) en el límite de n grande un número n de copias independientes de ψ, es decir ψ ⊗ n' pueden transformase por medio de operaciones locales y de comunicación clásica en un estado arbitrariamente cercano a ψ ⊗ n', donde la fidelidad de tiende a 1 y con (n'/n) → (E(ψ)/ E(ψ)).

Es interesante observar que la medida de entrelazamiento que hemos hecho es *aditiva*. Si Alice y Bob tienen subsistemas con entrelazamientos E_1 y E_2, entonces el sistema global que comparten tiene entrelazamiento $E_1 + E_2$.

La cantidad de entrelazamiento de estado puro que se necesita para crear un estado mezclado se sabe que es en general menor que la que se puede obtener de ese estado. A la primera cantidad la llamaremos *entrelazamiento de formación*, y a la segunda *entrelazamiento destilable*. A

nivel cuantitativo, la definición de entrelazamiento de formación involucra el número de pares Experimento de Pinten, Polosky y Rosen (EPR) necesarios para crear copias de un cierto estado con alta fidelidad, y la del entrelazamiento destilable, el número de pares EPR casi perfectos que se pueden obtener con elevada fiabilidad de las copias del estado.

2.6 Teoría de la Información Cuántica

2.6.1 Nociones básicas sobre información en mecánica cuántica.

Al principio comenté el hecho de que el tratamiento de la información como entidad independiente adquirió un nuevo significado a raíz del surgimiento de la mecánica cuántica. El apartado que comienza ahora no es más que un repaso sobre los conceptos más básicos de la física cuántica, pero por completitud he decidido incluirlo. Los postulados de la mecánica cuántica que nos interesan ahora son los siguientes:

1. El estado de un sistema aislado Q se representa por un vector | ψ (t)> en un espacio de Hilbert.
2. Las variables, tales como la posición y el momento se denominan *observables* y se representan por operadores herméticos. En la base de estados propios de X las componentes de la posición y el momento son:

$$\langle x \mid X \mid x' \rangle = x\,\delta(x - x')$$

$$\langle x \mid P \mid x' \rangle = -ih\,\delta'(x - x')$$

3. El vector de estado evoluciona de acuerdo a la ecuación de Schrödinger:

$$ih\,\frac{d}{dt}\psi(t) = H \mid \psi(t) >$$

Donde H es el operador hamiltoniano.

4. El estado de un sistema cuántico inmediatamente después de que sobre él se efectúe una medida es la proyección del estado anterior sobre el sub-espacio correspondiente al valor propio obtenido de ésta. En el caso de que este valor propio fuese no degenerado el resultado sería precisamente el vector propio correspondiente.

$$\psi'(\tau_o^+) \geq \sum_{i=1}^{gn} \; | \mathrm{U}_\mathrm{n}^\mathrm{i} >< \mathrm{U}_\mathrm{n}^\mathrm{i} \; | \psi(t_o^+) >$$

Donde no he utilizado el signo igual porque el miembro de la derecha está sin normalizar. Una consecuencia de los postulados es que la evolución de un sistema cuántico aislado siempre es unitaria:

$$| \psi(t) \geq \mathrm{U(t)} \psi(0) >$$

Con U, el operador de evolución, unitario:

$$\mathrm{U(t)} = \exp\left(- \frac{\mathrm{i}}{\mathrm{h}} \int H dt \right); UU^t = i >$$

Pero los sistemas aislados no existen. Modelizar cualquier sistema cuántico por medio de la Ec. Schrödinger implica hacer una aproximación más o menos fuerte. Un modo de tratar el problema de los alrededores es simplificándolos como un único sistema, Γ, que en cierto modo se comporta como si realizase una medida sobre el estado de Q. Las proyecciones asociadas a la interacción no son unitarias, así que aparece una contribución no unitaria en la evolución. Este fenómeno se conoce como *decoherencia*.

2.6.2 El problema de la simulación.

Después de recordar las herramientas que necesitaremos, se plantean las siguientes cuestiones:

1. Parece que la naturaleza funciona como un gran procesador de la información, y más a la luz de los postulados de la mecánica cuántica.

Un ket, como descriptor de un sistema cuántico en un instante de tiempo, es un paquete de información, y como tal se comporta. Contiene no la información total para especificar por completo el estado del sistema q, sino sólo la que hay disponible, y no información sobre otros sistemas.

2. ¿Puede una computadora simular a la naturaleza en conjunto? Convirtamos la conjetura de Church-Turing en un principio de la física:

Cualquier sistema físico finito realizable puede simularse con precisión arbitrariamente elevada por una computadora universal con un número finito de estados.

Observemos que el postulado no involucra máquinas de Turing. Hay grandes diferencias entre las máquinas de Turing y los principios que rigen el comportamiento de los sistemas cuánticos. La idea sobre la que gira la computación cuántica es la posibilidad de llevar a cabo nuevos tipos de cálculos, completamente distintos a los llevados a cabo por los computadores tradicionales. Y hay resultados que llevan a pensar que realmente existe tal posibilidad. El problema de la simulación fue tratado por Feynman en su famoso artículo de 1982, en el que también apuntó a la posibilidad de construir un computador basado en las leyes de la mecánica cuántica.

Un computador cuántico en principio parece obvio que serviría para simular sistemas cuánticos. Supongamos que pretendemos simular un sistema cuyo espacio de Hilbert sea de dimensión 2^n mediante un computador clásico. Está claro que necesitaremos 2^n números complejos, las componentes del vector de estado. Un computador cuántico, en cambio, requiere tan sólo de n qubits para hacer lo mismo. Así que a nivel de almacenamiento la ventaja de un computador cuántico sobre uno clásico es obvia. A nivel de cálculo, ni uno ni otro resultarán en general eficientes, pues mientras que para un computador clásico debemos manipular matrices de dimensión 2^n (lo que equivale a número de cálculos exponencial con el

tamaño de la entrada, n) un computador cuántico deberá realizar transformaciones unitarias sobre un espacio de 2^n dimensiones, cosa que necesitaría un número de puertas que crece en la misma medida.

Se demuestra que existen *algunos* sistemas para los que en efecto un computador cuántico puede proceder de manera más eficiente que uno clásico, si bien esta no es la situación general.

2.6.3 Primera sorpresa: Es posible medir sin alterar un sistema.

Consideremos parejas de sistemas cuánticos de dos estados, como partículas de spin 1/2. Llamemos a nuestras partículas A y B, y asociemos los números cuánticos del modo acostumbrado:

$$spinup: m_z = \frac{1}{2}; |\uparrow>$$

$$spindown\ m_z = \frac{1}{2}; |\downarrow>$$

Preparamos el sistema en el estado inicial:

$$|\psi(0)>= \frac{1}{\sqrt{2}}(|\uparrow>|\downarrow> - |\downarrow>|\uparrow>)$$

Entonces ambas partículas se mueven en sentidos opuestos a lo largo de un eje coordenado cualquiera, por ejemplo OY. Por un lado Alice recibe su partícula, y por otro lo hace Bob. El resultado permite predecir con certeza la medida de cualquier componente de s^B, sin perturbar a B. De este modo, las componentes del spin de B están definidas, y por tanto la descripción que hace la mecánica cuántica del sistema es incompleta.

Para hacer la predicción, escogemos cualquier eje η a lo largo del que nos gustaría conocer el momento angular de B. Pero en lugar de medir el spin de B medimos el de A, con un aparato de Stern-Gerlach, alineado con η. El spin del estado singlete que preparamos al principio era cero, de modo que por conservación del spin, el de B debe ser siempre opuesto al de A.

¿Dónde está el problema? Las alternativas habituales:

1. La medida que realiza Alice influye en el estado de la partícula que recibe Bob.

2. El vector de estado del sistema cuántico | ψ > no es una propiedad intrínseca del sistema cuántico, sino una expresión del contenido informativo de una variable cuántica. En el estado singlete hay información mutua entre A y B, de modo que el contenido informativo de B cambia cuando conocemos el valor de A. Desde este punto de vista el comportamiento puede describirse usando la teoría clásica de la información.

2.6.4 Segunda sorpresa: Las desigualdades de Bell.

Imaginemos que Alice y Bob miden spines a lo largo de distintos ejes, η A y η B, contenidos en el mismo plano, digamos XZ. Cada medida tiene dos resultados posibles: spin up , o spin down. Teoría y práctica coinciden en que la probabilidad de que el resultado encontrado por ambos sea el mismo es

$$P_{eq} = \sin^2((\phi A - \phi B)/2)$$

En la expresión ϕA y ϕB son los ángulos que forman respectivamente los ejes ηA y ηA con el eje OZ. Pero no hay manera de asignar propiedades locales a A y B independientemente. Al observar la ecuación de arriba vemos que en la probabilidad hay un altísimo grado de correlación. Lo que ocurre en B depende del ángulo ϕA, y al contrario. El máximo grado de correlación corresponde a $\phi A - \phi B = 120^{\circ}$, que da como resultado 2/3.

Este resultado permite imaginar una tarea que los computadores clásicos son incapaces de realizar: comunicar información más rápido de lo que permitiría una señal luminosa. A partir de ϕA y ϕB, comunicar señales binarias perfectamente correlacionadas con $\phi A = \phi B + 180$, anticorrelecionadas con $\phi A = \phi B$, y correlacionadas en más de un 70% con $\phi A - \phi B = 120^{\circ}$.

Estos resultados fueron comprobados en el laboratorio en los años 70 y 80. Estos últimos resultados nos colocan por fin en el lugar adecuado para estudiar la teoría cuántica de la información con un poco más de profundidad.

2.7 Quantum bits:

Definición 1 "un quanta bit para abreviarlo qubit, es un sistema cuantico de 2 niveles, Para no crear mucha confusión solo diremos, que dos dimensiones en el espacio de Hilbert H_2 es un qubit. H_2 contiene B = {|0>,|1>}, que lo llamaremos computación básica, los estados |0> y |1> son llamados los estados básicos".

El estado general de un qubit tiene un vector de longitud

$c_o|0> + c_1|1>$ Teniendo como unidad de medida $|c_o|^2 + |c_1|^2 = 1$

Nosotros podemos observar que un bit en estado de $c_o|0> + c_1|1>$ no puede generar un 0 o 1 dependiendo de la probabilidad de $|c_o|^2$ o $|c_1|^2$ respectivamente.

Definición 2 Un operacion de u qubit, llamada una puerta unitaria cuantica, es un mapeo unitarios U: $H_2 \rightarrow H_2$.

En otras palabras, una puerta unitaria cuantica define una operación lineal:

|0> →a|0>+ b|1>

|1> →c|0>+ d|1>

Donde la matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Es unitaria

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a* & b* \\ c* & d* \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

La notación

$$(a,b)^T = \begin{pmatrix} a \\ b \end{pmatrix}$$

Se usa para dar la matriz transpuesta.

2.8 Registros Cuanticos:

Un sistema de dos quantum bits es un espacio de hilbert de 4 dimensiones $H_4 = (H_2 \otimes H_2)$ teniendo ortonormal básico en {|0>|0>,|0>|1>,|1>|0>,|1>|1>}, también se puede escribir |0>|0> =|00>,|0>|1>= |01> etc. El estado de un sistema de 2 qubits tiene un vector de longitud igual a:

$c_o|00> + c_1|01> + c_2|10> + c_3|11>$

Teniendo como requerido $|c_o|^2+|c_1|^2 +|c_2|^2+ |c_3|^2=1$

Nótese que los estados no se pueden conmutar o sea |0>|1> ≠ |1>|0> , se tiene que usar orden linear (escribir e izquierda a derecha) cada qubit individualmente.

2.9 Maquina de Turin Cuatica:

La maquina de Turín cuantica se ejemplificara basándonos en la maquina de Turín probabilística, y generalizándola la probabilística, remplazando las funciones probabilísticas con transición de amplitudes. Basado en esto esta seria la función de transición de amplitud:

$\delta = Q \times A \times Q \times A \times \{-1,0,1\} \to C$

Donde $\delta(q_1, a_1, q_2, a_2, d)$ da la amplitud que como siempre la maquina este estado q_1 buscando el símbolo a_1, entonces se remplaza a_1 por a_2 ingresando el estado q_2 y moviéndose hacia delante en dirección de Є{-1,-0-1}.

Definición 3 Una maquina de Turín cuantica (QTM) por sus siglas en ingles, sobre A es un sextuple $(Q, A, \delta, q_0, q_a.q_r)$, donde $q_0, q_a.q_r \in Q$ son los estados inicial, de aceptación y de error. La función de transición de amplitud debe satisfacer

$$\sum_{(q_2,a_2,d)\in Q\times A\times\{-1,0,1\}} \left|\delta(q_1,a_1,q_2,a_2,d)\right|^2 = 1$$

Para todo $(q_1, a_1) \in Q \times A$

2.10 Circuitos Cuánticos

Recordemos que la Maquina de Turín pude hacer cómputos parciales de la definición de f : A→A. Entonces nosotros podemos Modificar A=F={0,1} para se un alfabeto binario y con ello considerar la función de un circuito booleano no cuantico como $\{0,1\}^n \to \{0,1\}^m$. Este es el elemento básico de estos circuitos ahora podemos escoger la función: Λ: $F_2^2 \to F_2$ (compuerta lógica and) definida por $\Lambda(x_1,x_2)=1$ si y solo si $x_1 = x_2 = 1$; V: $F_2^2 \to F_2$ (compuerta lógica 0r) definida por $V(x_1,x_2)=0$ si y solo si $x_1 = x_2 = 1$; y la compuerta lógica not $F_2^2 \to F_2$ definida por ¬X= 1-X.

Un circuito boleano es un grafo dirigido no cíclico, que los nodos son etiquetados cada uno con variables de entrada, variables de salida, o compuertas lógicas Λ, V y ¬. Y los nodos de la variables de entradas no tiene conectores (flechas →) de ingreso a ellos, mientras que las variables de salida no tiene conectores de salida (flechas →) . Los nodos con compuertas Λ, V y ¬ solo pueden tener 2,2,1 fechas de ingreso respectivamente (flechas →) y las conexiones del grafo es llamada dirigida o alambrada. El número de nodos de un circuito es llamado complejidad del circuito booleano.

Un circuito booleano con n variables de entrada x_1 ,….., x_n y m de salida $y_1,\ldots,y_m$ naturalmente definido dentro de la función $F_2^n \rightarrow F_2^m$: las sentadas están codificadas dando la variables de entrada 0 y 1, a cada compuerta y una función primitiva Λ, V y ¬. El valor de la función esta dado en la secuencia de las variables de salida $y_1,\ldots,y_m$.

Ahora un circuito cuantico lo podemos identificar nuevamente como una cadena de bits $x \in F^m_2$ and un ortogonal básico $\{|x\rangle \; |x \in F^m_2\}$ de un 2^m dimensiones espacio de Hilbert H_2^m. Para representar el mapa lineal de $F^m_2 \rightarrow F^m_2$ adoptaremos una representación coordinada $|x\rangle = e_i = (0,\ldots..1,\ldots,0)^T$, donde e_i es una columna del vector teniendo 0 en cualquier caso pero 1 in la posición i-esima, si los componentes de $x = (x_{1,} \ldots\ldots., x_m)$ de una representación binaria del numero i+1.

Una puerta reversible f en m bits es una permutación de F^m_2 esto quiere decir que una compuerta reversible solo puede definir un mapeo lineal en H_2^m , Esto es una permutación de $2^m \; X \; 2^m$ de la matriz $M(f)$[12] representado este mapeo, $M(f)_{ij}=1$ si $f(e_j) = e_i$ y $M(f)_{ij}=0$ en otros casos.

Definición 4 Una compuerta cuantica en m qubits is un mapeo unitario en $H_2 \otimes ... \otimes H_2$ (m veces), con operadores con de números reales (independientes de m) de qubits.

Por que M(f)*$_{ij}$=1si y solo si f (e_j) = e_i y M(f)* representa la permutación inversa de f . Entonces, una matriz de permutaciones es siempre unitaria y las compuertas reversibles son un caso especial de las compuertas cuanticas. La noción de circuito quántico es sacando de un circuito reversible que es reemplazado por las compuertas reversibles por compuertas quánticas. La única diferencia entre compuertas cuantias y circuitos quánticos es solo contexto: requerimos que el circuito quántico este compuesto por compuertas quánticas las cuales operan en un numero limitado de qbits

Definición 5 Un circuito quántico de m qubits es un mapeo unitario en H_2^m, que podemos representar como una concatenación de un set finito de compuertas de compuertas quánticas.

Desde que circuitos reversibles son también circuitos quánticos, pudimos descubrir el hecho que cualquier cosa que sea computable por una circuito booleano es computable por un circuito quántico.

2.11 La transformada de Furrier Cuántica

Sea G = {g1,g2,...,gn} un grupo abeliano (se usara notación aditiva) y sea {x1,x2,...,xn} los caracteres de G. Las funciones f: G $\rightarrow$ C forman un vector de espacio complejo V, la adición y multiplicación escalar están definidas puntualmente. Si f1,f2 $\in$ V, entonces el producto interno estándar de f1 y f2 esta definido por:

$$\langle f_1 \mid f_2 \rangle = \sum_{k=1}^{n} f_1^n(g_k) f_2(g_k)$$

Cualquier producto interno induce una norma por ||f|| = √<f|f>. En la sección 8.2 esta demostrado que las funciones Bi = (1/√n) xi forman una base ortonormal del vector espacio, así que cada f ∈ V puede ser representado como:

f = c1B1 + c2B2+...+cnBn,

Donde ci son los números complejos llamados los coeficientes de fourier de f. La transformada discreta de fourier de f ∈ V es otra función f^ ∈V definida por f^(gi) = ci. Como las funciones Bi forman una base ortonormal , vemos fácilmente que ci = <Bi | f>, así que

$$\hat{f}(g_i) = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} x_1^n(g_k) f(g_k)$$

A

La transformada de fourier satisface la identidad de Parseval

$$\| \hat{f} \| = \| f \|$$

La cual será importante en la secuela

Sea H un sistema quántico finito capaz de representar elementos de G. Esto significa que {|g> |g ∈ G} es una base ortonormal de algún sistema quántico H . Para obtener las representaciones matriciales para mapeo lineal, usamos representación por coordenadas |gi> ei = $(0,...,1,...,0)^T$ (todas las coordenadas son 0 excepto el 1 en la iesima posición; vea sección 8.3) los estados generales del sistema son combinaciones lineales de longitud unitaria de los estados bases. Además un estado general

$$C_1|g_1\rangle + c_2|g_2\rangle + \ldots\ldots + c_n|g_n\rangle$$

de H puede ser visto como mapeo

$$f : \mathrm{G} = \mathrm{C}, \quad \text{where } f(g_i) = \mathrm{c}_1 \quad \text{and } \| \mathrm{f} \| = 1,$$

y viceversa, cada mapeo define un estado de H.

Definición 6 *La transformada quántica de fourier (QFT) es la operación:*

$$\sum_{k=1}^{n} f(g_k) \mid g \; > \rightarrow \sum_{k=1}^{n} \hat{f}(g_k) \mid g \; >$$

En Otras palabras, la transformada quántica de fourier es solamente la transformada de fourier ordinaria de una función f: G $\rightarrow$ C determinada por las operaciones anteriores y que la cobierten en

$$g_i > \rightarrow \frac{1}{\sqrt{n}} \sum_{k=1}^{n} x_k^i(g_i) \mid g_k >,$$

y entonces es claro que en la base $\mid$gi>, la matriz de la transformada quántica de fourier es:

$$\frac{1}{\sqrt{n}} \begin{pmatrix} x_1(g_1) & x_1(g_2) & .... & x_1(g_n) \\ x_2(g_1) & x_1(g_2) & .... & x_1(g_n) \\ & & & \\ x_n(g_1) & x_n(g_2) & .... & x_n(g_n) \end{pmatrix}$$

¿Que clase de circuito quántico se necesita para implementar la ecuancion presentada antes de la matriz de arriba? el problema que se presenta es que, en una típica situación, n = $\mid$G$\mid$ = dim (H) es grande, pero usualmente H es un producto tensor de espacios menores. Sin embargo, unas operaciones de circuitos quánticos se requiere que sean locales, sin afectar un gran numero de dígitos quánticos al mismo tiempo. En otras palabras, el problema es como podemos descomponer la matriz QFT de arriba en un producto tensor de matrices pequeñas, o en producto de unas cuantas matrices que puedan ser expresadas como un producto tensor de matrices operando solo en algunos sub-espacios pequeños.

Para aproximarnos a este problema, asumamos que G = U $\oplus$ V es la suma directa de los subgrupos U y V. Sea r = $\mid$U$\mid$ y s = $\mid$V$\mid$, entonces $\mid$G$\mid$

= rs. Sean también U y V representados por algunos sistemas Hu y Hv con bases ortonormales:

$$\{|u_1>.....|U_r>\} \text{ and } \{|V_1>.....|V_r>\}$$

Respectivamente. Entonces, el producto tensor Hu $\oplus$ Hv representa a G en una forma muy natural: cada g $\in$ G puede ser expresado de forma única como g = u +v, donde u $\in$ U y v $\in$ V, así que representamos a g = u+v por $|u>|v>$. Como tenemos una descomposición G = U * V, todos los caracteres de G pueden ser escritos como:

$$X_{ij}(g) = x_{ij}(u + v) = x^{U}_{i}(u)x^{V}_{j}(v)$$

Donde Xi^{u} y $Xj^{v}(u)$ son caracteres de U y V respectivamente y:

$$(i,j) \in \{1,....,r\}x\{1,.....,s\}$$

Además, la transformada de fourier puede ser descompuesta.

TEOREMA 1 (descomposición de la transformada de fourier) Sea G = U $\oplus$ V un producto directo de los subgrupos U y V y $\{|u>|v> \; | u \in U , v \in V\}$ una representación cuántica de los elementos de G. Entonces

$$|U^{i}_{i}>|V_{i}> \rightarrow \left(\frac{1}{\sqrt{n}}\sum_{k=1}^{n} x^{u}_{i}(u_k))^{*}|u_{k)}\right)\left(\frac{1}{\sqrt{s}}\sum_{t=1}^{s} x^{v}_{j}(v_t)^{*}|v_k\right)$$

$$= \frac{1}{\sqrt{rs}}\sum_{k=1}^{n}{}^{i}\sum_{k=1}^{n} x^{i}_{k}(u_k + v_t)|U_k>|V_t> \quad (4)$$

Es la transformada de Fourier de G

La descomposición de la transformada de fourier puede ser aplicada recursivamente a los grupos U y V es también interesante notar que el estado (4) es descomponible.

2.12 Algoritmos de Búsqueda Cuánticos

2.12.1 Los problemas que resuelve el computador cuántico.

De entrada hemos descubierto que el computador cuántico no es aquella panacea capaz de resolver todos los problemas que se nos ocurran. Existe aquel grupo de problemas que es irresoluble por naturaleza, como el de la detención. Sin embargo, tenemos una ventaja enorme cuando hablamos de mecánica cuántica: El espacio de los estados crece exponencialmente con el número de qubits, mientras que lo hace linealmente con el número de bits. Esto se debe a que si bien n bits pueden combinarse de 2^n maneras diferentes, una combinación de n qbits admite todas las combinaciones lineales posibles de vectores de estado, cada uno de los cuales supone a su vez las 2^n combinaciones.

Mejor que hablar tanto será tratar de ilustrarlo con un ejemplo. Lo natural será escoger el caso más sencillo: 2 qubits frente a dos bits. Los estados posibles fruto de la combinación de 2 bits son:

x_1x_2= 00;01;10;11

Es decir $2^2 = 4$estados. Ahora veamos qué ocurre si disponemos de 2 qubits. En principio parece evidente que disponemos de estos estados:

$$\{|q_1,q_2>\}=\{|0,0>;|0,1>;|1,0>;|1,1>]$$

Pero esto es sólo la base. Esto es, *la dimensión del espacio* ha crecido exponencialmente con el número de bits. En este espacio es posible encontrar toda clase de combinaciones de elementos de la base:

$$|\Phi>=\alpha|g_1\ g_2>+b|g'_1\ g'_2>$$

Siempre que esté normalizada. Si hablamos de partículas idénticas estos estados deben ser de simetría bien definida. Es habitual trabajar con electrones (fermiones), por lo que los estados posibles serán antisimétricos, o fotones (bosones) para los que los estados posibles son simétricos. Los qubits, desde un punto de vista intuitivo da la impresión de que son capaces de barrer muchos casos posibles con una cantidad de recursos que no sería ni de lejos suficiente para un computador electrónico. Esto, que he dicho de un modo tan informal, veremos que se traduce en hechos, como los métodos de Shor y de Grover. Por un lado, el primero es capaz de encontrar la descomposición en factores primos de un número en un tiempo que crece linealmente con el tamaño del número a factorizar, aprovechando el crecimiento exponencial de la dimensión del espacio con el que se trabaja. En un computador clásico el tiempo vimos que crece exponencialmente con el tamaño de la entrada. El algoritmo de búsqueda de Grover, por otra parte, tiene propiedades similares en lo que se refiere a buscar elementos determinados en listas grandes, donde los tiempos de búsqueda son también mucho mayores en los computadores clásicos.

En principio, la conclusión es que la mecánica cuántica es un herramienta muy poderosa de aceleración de cálculos, y poco más. Pero esto no es trivial, desde el momento que vemos que esta aceleración puede ser exponencial, y por tanto saca problemas del dominio irresoluble al dominio p. El entrelazamiento hace posibles algunas otras cosas también. Estas son algunas aplicaciones interesantes.

2.12.2 El método de factorización de Shor.

Los métodos modernos para descomponer números grandes en factores primos son considerados ineficientes, y no permiten en general obtener descomposiciones en tiempos razonables. Este problema, aún bastante particular, resulta de gran interés, y tiene solución conocida en el campo de la computación cuántica. Existen otros muchos problemas donde

un QC es más eficiente que un computador clásico, la mayoría de ellos sin descubrir. Esto constituye un campo de búsqueda activo.
Ocupémonos de los algoritmos de *búsqueda del periodo de una función* y, como caso particular, *des-compocisión en factores primos.*

2.12.3 Búsqueda del periodo de una función.

Partamos de la función f(x), cuyo periodo es r:

$$f(x+r)=f(x)$$

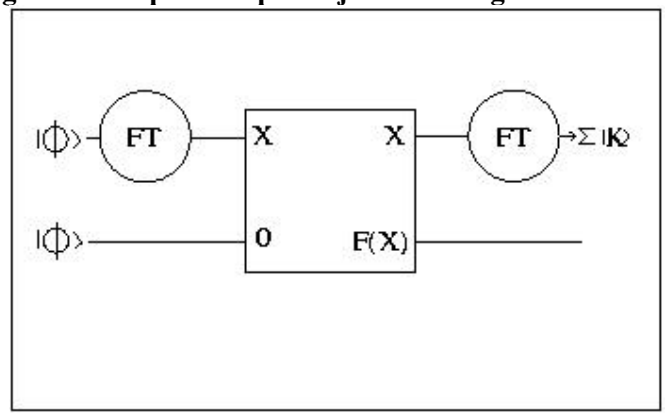
Partamos de dos suposiciones adicionales: f(x) puede computarse eficientemente en x, y sabemos que r cumple:

$$\frac{n}{2} > r < N$$

para un N dado. En un computador clásico, en ausencia de un método analítico para hallar el periodo de la función, lo mejor que podemos hacer es evaluar f(x) en alrededor de N/2 puntos, y buscar dónde comienzan a repetirse los resultados. El número de operaciones crece exponencialmente con log N, que es la información necesaria para especificar N.

En la siguiente figura muestro el modo en que un QC resolvería el problema:

Figura 13 Dispositivo para ejecutar el algoritmo de Shor



Los requisitos para ejecutar el algoritmo son 2n qubits, más del orden de n más para almacenamiento intermedio (espacio de trabajo), con n=[2logN], donde el símbolo [….] significa ``el entero inmediatamente superior'' al argumento.

Utilizaremos dos registros de n qbits cada uno, que llamaremos **x** e **y.** Prepararemos ambos registros en el estado inicial |0>.

Aplicaremos la operación H (transformada de Fourier) a cada qubit del registro **x**. El estado obtenido:

$$\frac{1}{\sqrt{w}}\sum_{x=0}^{w-1}|\ x\ >|\ 0\ >:\ w\ =\ 2^{n} \qquad (5)$$

Donde |x> significa, por ejemplo, |0011001>, con 0011001 la representación binaria de **x**. Denominamos a {|0>,|1>} la *base computacional*.

Hacemos entonces pasar los registros **x** e **y** por una red de puertas de modo que se efectúe la transformación

$$U_f\left(\frac{1}{\sqrt{w}}\sum_{x=0}^{w-1}|\ x>|\ 0>\right)=\frac{1}{\sqrt{w}}\sum_{x=0}^{w-1}|\ x>|\ f(x)>$$

Este proceso es reversible, dado que el estado del miembro derecho está biunívocamente determinado por el del miembro izquierdo, de modo que U_f puede ser una transformación unitaria.

Hemos obtenido el valor de $f(x)$ para $\omega\ =\ 2^{n}$ valores de una sola vez. Esto se conoce como *parlelismo cuántico*. La dependencia con n es exponencial, de modo que el grado de paralelismo es enorme. Con sólo n=100 tenemos 2^{100} ≈N procesadores clásicos.

Nos enfrentamos al inconveniente de no tener un modo directo de alcanzar los valores almacenados en el estado 38. Un modo de obtener información es medir los estados del registro **y**, donde almacenamos $f(x)$, pero eso sólo nos dará un valor de f, debido al colapso del estado en el

sub-espacio correspondiente al auto-valor medido. Imaginemos que hemos medido el registro **y**, y obtuvimos $f(x) = \upsilon$. Entoces todo el registro **y** colapsará en el estado |u> , asociado a un valor determinado para todas las componentes del registro. Pero sabemos que en el registro hay información sobre 2^n evaluaciones de f. El estado total sería:

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{m-1} | du + jr > | u >$$

Donde $d_u + j_r$, con j=0,1,2...M-1 son todos los valores de **x** para los que f(x) = u. El periodo de f(x) conlleva que en el registro **x** aparece una superposición de M ≈ w/r estados, con valores de x separados un periodo r. El offset es d_u, y depende del valor de u obtenido al medir el registro **y**.

Lo único que queda es extraer la periodicidad del estado contenido en el registro **x**. Esto se hace directamente, haciendo la transformada de Fourier del estado, y midiendo a continuación. La transformada de Fourier discreta es la siguiente operación:

$$U_{.FT} \mid x >= \frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} \mid e^{i 2\pi kx / w} \mid k >$$

Conviene observar en este momento que la operación 5 es un ejemplo de transformada de Fourier, como dije antes sin justificar, donde se actúa sobre el estado |0>. Hemos supuesto que r es un divisor de □, de modo que M= □ /r es una división exacta. Esta simplificación puede hacerse innecesaria.

En lo sucesivo no nos interesa lo que haya almacenado en el registro **y**. La aplicación del operador U_{FT} sobre el estado del registro **x**:

$$U_{.FT} = \frac{1}{\sqrt{w/r}} \sum_{x=0}^{w-1} \mid du + jr >= \frac{1}{\sqrt{r}} \sum \mid k \, \hat{f}(k) \mid k >$$

donde

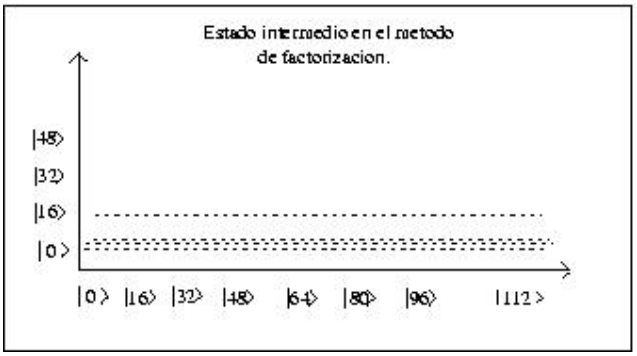
$$|\hat{f}(k)| = \begin{Bmatrix} 1...; k...esmultiplo\ \ de...w/r \\ 0..... .; losdemasca\ \ sos \end{Bmatrix}$$

Ahora queda obtener el valor de r (el periodo) a partir del resultado. Sabemos que x= $\lambda\ \omega$/r, con λdesconocido. Si λy r no tienen factores comunes podremos despejar x/ω , que será una fracción irreducible, y a partir de ella y de x, obtener tanto r como λ. Si λy r tienen algún factor común, cosa poco probable para valores grandes de r, el algoritmo falla, y debemos repetir todos los pasos desde el principio. Tras un número de repeticiones del orden de log r la probabilidad de obtener el resultado correcto se hace tan alta como queramos.

Observamos que el límite de eficiencia del método de Shor viene dado por la evaluación de $f(x)$. Por contra, el número de puertas lógicas requeridas para la búsqueda del periodo crece polinómicamente en n, en lugar de hacerlo exponencialmente.

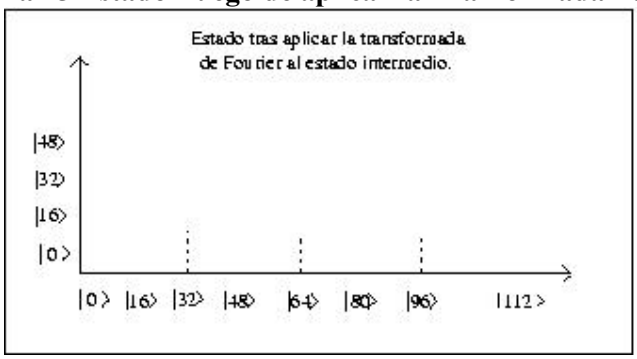
Los pasos intermedios vienen representados en estas figuras:

Figura 14 Estado intermedio en el metodo de Factorizacion



Primera etapa

Figura 15 Estado Luego de aplicar la Tranformada Furier



2.12.4 Teletransporte cuántico.

El teletransporte es en esencia lo que su propio nombre indica. Puede no ser necesario enviar un qubit para hacer llegar información de un punto a otro.

Alice está interesada en hacer saber a Bob el valor de un qubit particular, digamos |Φ>=|0>, que ella conoce. No necesariamente hay que hacer llegar el qubit |0> hasta Bob. La posibilidad que pasa por medir antes el qubit, de todas formas, en caso de que éste fuera desconocido para Alice, y de enviar despues la información destruiría el estado inicial. Y ya sabemos que no se puede copiar un estado que no es conocido. Así que Alice siempre conoce el estado del qubit.

El teletransporte cuántico utiliza el entrelazamiento para resolver estas dificultades.

Supongamos que Alice y Bob comparten un par entrelazado en el estado $(|00>+|11>)/\sqrt{2}$. Alice pretende transmitir a Bob un qubit en un estado *desconocido.* Este estado será representado como

$$| \Phi >= \alpha|0> + b|1>$$

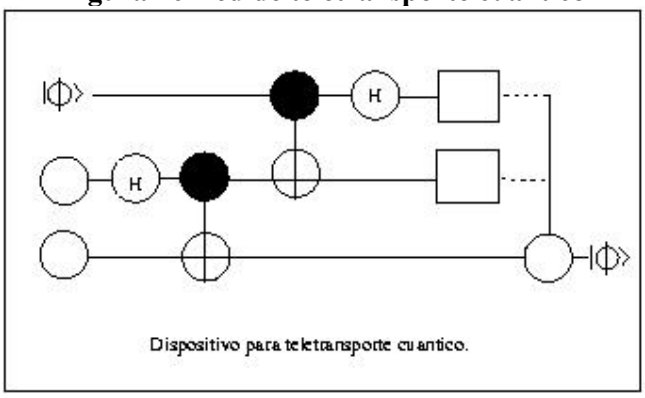
El estado inicial de los tres qubits será:

$$\left[a\,|\,0>+b\,|\,1>\right]\otimes\frac{1}{\sqrt{2}}\left[|\,00>+|\,11>\right]=$$

$$=a\,|\,000>+\beta\,|\,100>+a\,|\,011>+\beta\,|\,111>$$

Desde luego, normalizado. Alice mide en la base de Bell (apartado anterior) los primeros dos qubits, que son aquél que es en principio desconocido, y que se desea transmitir, y su parte del par entrelazado. Esto se puede hacer mediante el esquema de la figura:

Figura 16 Red de teletransporte cuántico



Dispositivo para teletransporte cuantico.

Primero Alice aplica las operaciones XOR y de Hadamard, y despues de esto el estado resultante es:

$$=|\,00>(a\,|\,0>+\beta\,|\,1>)+|\,01(a\,|\,1>+\beta\,|\,1>+$$

$$+|\,10>(a\,|\,0>+\beta\,|\,1>)+|\,00>(a\,|\,1>+\beta\,|\,1>)$$

Inmediatamente después mide sus qubits. De acuerdo al postulado de la medida, el estado inmediatamente a continuación de ésta es el colapso

sobre uno de los cuatro estados de la base de Bell, que contiene dos bits de información. Enviamos estos dos bits a Bob, que con ellos será capaz de decidir que operación {I,X,Y,Z} debe aplicar a su qubit, para pasarlo al estado $|\phi>$ =a|0>+b|1>. Así Bob ha sido capaz de recuperar el qubit sin que éste fuese en sí transmitido.

No es posible clonar un estado que no se conoce, y no se ha podido hacer llegar a Bob el qubit sin que Alice lo perdiese. Por otra parte, $|\phi>$ contiene información completa sobre el estado del qubit de Alice, de modo que no se ha perdido información. De estos dos hechos se deriva que el término *teletransporte* sea adecuado para esta situación.

2.13 Algoritmos de búsqueda

2.13.1 El algoritmo de búsqueda de Grover.

Otra aplicación de la potencia de la mecánica cuántica en la resolución de problemas computacionalmente pesados es la búsqueda de elementos en listas. El método es una variante del de búsqueda del periodo de una función. Nos ocupamos de listas desordenadas, que es donde un sistema clásico de búsqueda no tiene más remedio que recorrerlas de algún modo buscando el elemento por medio de repetidas comparaciones. Existen diferentes alternativas, que mejoran la eficiencia de las búsquedas, pero cada una de ellas parte de situaciones particulares en las que rentabiliza el número de operaciones. Un ejemplo relativo a la seguridad informática: una lista de contraseñas habitualmente se almacena encriptada en algún archivo de sistema, de modo que cuando cualquier usuario teclea su contraseña esta se encripta de nuevo (con un coste computacional insignificante) y se compara con la versión encriptada de la lista. Desencriptar una contraseña codificada por ejemplo vía RSA, es actualmente un problema inabordable cuando la clave es suficientemente compleja. Las personas que pretenden

acceder a un sistema protegido de esta manera sin permiso habitualmente optan por hacer un ataque por *fuerza bruta,* esto es, recorrer todas las combinaciones posibles de caracteres una por una hasta encontrar una que sea una contraseña. Esta búsqueda a menudo se enfoca de un modo diferente: teniendo en cuenta que muchas personas utilizan palabras con sentido en algún idioma, utilizan *diccionarios*, que no son otra cosa que bases de datos de palabras en algún idioma, que lleva mucho menos tiempo recorrer, de modo que por regla general el coste computacional de romper la seguridad de un sistema informático puede disminuir considerablemente. *Si* estas condiciones se rompen el algoritmo puede hacerse muy ineficiente. De esta forma, si ningún usuario utiliza una clave basada en lenguaje natural el intruso recorrerá el diccionario completo sin obtener resultados satisfactorios.

Del ejemplo anterior extraemos la siguiente conclusión: si no sabemos nada sobre una lista no hay motivo para escoger un enfoque en lugar de otro, salvo el de maximizar las posibilidades de éxito. Esto incluso conlleva hacer más pesada la computación, pues nos obliga a hacer todas las comparaciones posibles.

Desde la perspectiva de la mecánica cuántica podemos utilizar el algoritmo presentado por Grover en 1997. El problema que resuelve puede representarse del siguiente modo:

Partimos de una lista desordenada $\{xi\]^{n}_{i}=1$, en la que tratamos de localizar un elemento particular, $X_i = t$.

Si bien un algoritmo clásico, recorriendo una lista de N elementos requiere en promedio realizar N/2 comparaciones, el método de Grover necesitará sólo hacer $\sqrt{n}$. El método no supone trasladar el problema a una nueva clase en el sentido de peso de computación, pero sí supone una aceleración tanto más significativa cuanto mayor sea la lista.

2.13.2 Algoritmo paso a paso:

Suponemos cada elemento de la lista etiquetado con un índice i, como expresé en el planteamiento del problema. Suponemos también que hay una operación unitaria que permite saber si el elemento actual es el que estamos buscando. El operador aplicado se denota por S:

S | i> =| i> ; i ≠ j

S | i> = - | j>; i = j

Donde j representa el índice del elemento buscado. Observemos que una estrategia para la resolución de problemas pesados es hacer una búsqueda aleatoria donde por comparación tratamos de determinar si cierto elemento es una solución al problema. Esto es el ejemplo que presenté en la introducción, o puede ser la búsqueda de la solución de una ecuación diferencial suponiendo buen comportamiento de las funciones implicadas.

Al igual que en el método de búsqueda del periodo, inicializamos un registro en una superposición de estados:

$$|\psi(\theta)>=\sin\theta\,|\,j>+\frac{\cos\theta}{\sqrt{N-1}}\sum\nolimits_{i\neq j}|\,i>$$

Los índices siguen correspondiendo a lo indicado en el paso (1). Este estado superpone con igual peso todos los elementos de la lista, pues partimos de $\theta_0=\frac{1}{\sqrt{N}}$. No decimos nada, sólo preparamos un registro donde todos los elementos están igualmente representados, tanto el que buscamos como los demás. De hecho, como el que estamos buscando es en principio un elemento cualquiera, simplemente hemos construido el

estado $|\psi>=(\frac{1}{\sqrt{N}}\sum_k|k>)$, donde los vectores |k> barren toda la lista. Nótese que el subíndice indica estado *inicial*.

A continuación aplicaremos el operador unitario S, que invertirá el signo del elemento que estamos buscando.

Por último, aplicamos la transformada de Fourier al estado resultante, lo que invierte el signo de todas las componentes excepto |0>. Entonces aplicamos de nuevo la transformada de Fourier. El efecto de esta secuencia de transformaciones, expresado en un único operador:

$$U_G|\theta>=\psi(\theta+\phi)>$$

donde. $\sin\phi=2\sqrt{n-\frac{1}{\sqrt{N}}}$

Encontramos que el coeficiente del elemento que buscamos es ligeramente mayor que el de los demás elementos de la superposición.

Sabiendo lo anterior, aplicaremos el operador U_G m veces, con $m=(\pi/4)\sqrt{N}$. Poco a poco el ángulo θ se va acercando a $\pi/2$, lo que hace cada vez más importante el coeficiente de |j> en la superposición, es decir, cada vez nos acercaremos más al elemento |j>.

Tras m iteraciones la probabilidad de error al medir el registro es del orden de N^{-1}.

Sólo hay un problema: aplicar demasiadas veces la transformación U_G disminuye la probabilidad de éxito. Para evitarlo debemos conocer m, es decir, el tamaño de la lista.

2.14 Búsqueda 'Instantánea' de Internet

Una aplicación práctica para tal algoritmo de búsqueda podría ser el aumento de la velocidad para encontrar una palabra escondida entre todos los datos almacenados en la red mundial de Internet, dice. No hace mucho,

los investigadores de IBM hicieron una especie de instantánea de toda la red, más de ocho billones de bytes en datos. Para buscar la palabra utilizando un ordenador convencional se precisaría todo un mes. Pero utilizando un ordenador cuántico sencillo sólo se necesitarían 27 minutos.

Los investigadores estudian ya la posibilidad de *coprocesadores cuánticos* similares a los coprocesadores matemáticos y aceleradores de gráficos de uso específico de los ordenadores personales utilizados hoy en día.

Para números con 130 dígitos encontramos que un computador cuántico no aporta ventajas sobre uno clásico (unas 7 horas con una tasa de conmutación del orden de un MHz), pero con 260 dígitos un computador que ejecutara el algoritmo anteriormente descrito tardaría 8 veces más, mientras que para un computador clásico el problema se hace intratable.

2.14 The Oracle

En el tiempo de la computadoras tradicionales, existen muchos problemas que por capacidad de procesamiento paralelos los tomamos como algoritmos que nunca se podrán tratar o solucionar.

Esto cono la computación cuantica ha dejado de ser un mito, pues hay problemas que de días o meses de procesamiento necesario han llegado a se calculados.

Esto esta ya en curso de investigación en cuanto tengamos ya computadores cuanticos de más de 4 o 5 qubits que son los que existen ahora, ya los problemas muy lentos o que no tenían solución podrán empezar a poder ser tratados y solucionado.

2.16 Performance

El performace que este modelo de computadora o computos nos da, nos lleva a pensar que con las limitantes que tenemos en este momento y ya se pueden hacer operaciones que antes no había forma de poder llevar a cabo dentro de la computación normal, deberá de ser mucho muy grande.

Solo en la definición de los qubits nos damos cuenta que el hecho de poder tener un qubit en un estado y otro a la vez nos da un performance de mejoramiento de tiempo de la mitad, ya definiendo mas de 1 qubit seguirá creciendo exponencialmente el performance.

2.17 Optimización de Algoritmos de Búsqueda

El programa de clasificación con el que trabajaron se conoce como algoritmo Grover de búsqueda. Es semejante a abrir cuatro puertas diferentes para encontrar un balón escondido tras una de ellas. Con un ordenador convencional sería necesario abrir, por término medio, más de dos puertas para encontrar el balón. Un ordenador cuántico, es capaz de abrir las cuatro puertas y localizar el balón en un solo paso.

Con esto podemos comprobar que cualquier algoritmo de búsqueda que existe dentro de lo que deberá de ser mucho mas rápido, debido al paralelismos que este modelo de computadora tiene inmerso en ella.

3 INFORMACIÓN CUÁNTICA

3.1 Ruido Cuántico

El ruido cuántico es el producto de la conversión del sistema fotónico al sistema eléctrico. Está compuesto por ligeras variaciones producto de este cambio.

Dada la continua mejora de las técnicas experimentales, el estudio del ruido cuántico ha dejado de ser una cuestión meramente teórica para convertirse cada vez más en un tema de carácter práctico.

De hecho el ruido cuántico es en la actualidad la fuente más importante de indeterminación en muchos montajes cuanticos. Entre ello se encuentra el montaje esquematizado en la figura diseñado para la detección pequeñas fuerzas.

Se trata de un interferómetro de Michelson en el que uno de los espejos puede moverse bajo la acción de la fuerza que se pretende detectar, movimiento que se traduce en un cambio en la intensidad que abandona el interferómetro. En este montaje la naturaleza cuántica de la radiación da lugar a dos fuentes de ruido.

Una son las fluctuaciones en el número de fotones registrados a la salida del interferómetro (ruido de recuento de fotones), que dan lugar a indeterminación en la posición del espejo. Otra fuente de ruido son las fluctuaciones de la presión de radiación, que causan fluctuaciones en la posición del espejo móvil.

En un principio las contribuciones de estas dos fuentes de ruido fueron calculadas como efectos estadísticamente independientes, con el resultado de que había un límite cuántico insuperable a la precisión con que se puede determinar la posición del espejo, el límite cuántico estándar.

La aportación en este tema parte de notar que ambas fuentes de ruido no pueden ser estadísticamente independientes, porque los campos dentro y fuera del interferómetro están necesariamente correlacionados. Además en este experimento sólo se mide una magnitud, la intensidad de salida, que debe contener toda la información de la medida.

Por lo tanto toda la incertidumbre de la medida debe derivarse de un ruido de recuento de fotones, tanto teórica como experimentalmente.

Para evitar estas dificultades incorporamos la movilidad del espejo en la transformación entrada salida del interferómetro incluyendo explícitamente en la transformación el hecho de que la longitud del brazo en el que está el espejo móvil depende de la intensidad de luz incidente sobre él.

El resultado es una transformación entrada-salida no lineal. Tras esto, toda la indeterminación en la posición del espejo se calcula en términos del ruido de recuento de fotones. De este modo hemos podido demostrar que, contrariamente a lo que se creía, no hay límite cuántico a la precisión de la medida

3.2 Corrección de Errores Cuánticos

3.2.1 Códigos cuánticos de detección de error

En conexión con la sección códigos correctores de error (detección de errores) comenzaré definiendo la matriz de chequeo de paridad. Decimos que un código detector de errores es lineal si es cerrado ante la suma:

$$u + v \in C, \forall u, v \in C$$

Un código de este tipo queda totalmente especificado por su matriz de chequeo de paridad, H, que es un conjunto de n-k palabras de bits line almente independientes, que satisfacen:

$$H.u = 0, \forall u \in C$$

Esto se traduce en la práctica en:

$$H.(u + e) = H.u + H.e = H.e$$

Al último término se lo denomina síntoma de error, y la clave de la idea es que delata el hecho de que un error se produjo sin necesidad de que Bob lea el mensaje (u), cosa que lo alteraría. De modo automático puede sustraerse el vector de error identificado, e, del mensaje original sin que por ello sea necesario leerlo en ningun momento.

Ahora pasaré de este nivel de formalidad a algo mucho más concreto. En primer lugar, la idea de introducir redundancia en los mensajes transmitidos tropieza con el teorema de no clonación. Si bien podemos pensar en un emisor que preparase múltiples copias de un cierto estado cuántico, en el proceso de medida el receptor no tendría modo de comparar cada no de estos estados con los demás, pues al medirlos los echaría a perder, y distintos estados cuánticos conducen a idénticas probabilidades para cada valor propio, como ocurre con

$$(1/\sqrt{2})(|0>+|1>) \text{ y } (1/\sqrt{2})(|0>-|1>)$$

Reproduciré el ejemplo empleado por Bennett y Shor para describir cómo se construyen los códigos cuánticos detectores de error. Primero partamos de la idea clásica de que para corregir un error basta repetir la información:

$$|0> \rightarrow |000$$

$$|1> \rightarrow |111$$

Si sólo hubiésemos duplicado la información, al producirse un error no sabríamos cuál de las alternativas es la correcta, mientras que aquí podemos suponer que la información correcta es la que aparece más veces. Aquí no enviamos varios estados, sino que empaquetamos el estado original (perteneciente a un espacio de dimensión 2) en un espacio de Hilbert de dimensión más elevada (8, en particular). La medida se hará una sola vez, y no tropezaremos con la imposibilidad de clonar el estado. Este código ya evita el único error que nos preocupa de la información clásica (esto es, la inversión de bits). Si en una comunicación se produce el error |0> ->|1> , este código será capaz de resolverlo. Pero la principal fuente de potencia computacional de la mecánica cuántica reside en el entrelazamiento, lo que quiere decir que esperamos conservar la fase de cada qubit en los estados que contienen la información. Una inversión de bit puede representarse por la aplicación del operador:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

que hace la transformación |0> -> |1> y |1> ->|0>. Si se produce por ejemplo una inversión de fase en el qubit |1>:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Tendremos un cambio de fase en la palabra completa. El código descrito en la ecuación 50 ha incrementado la vulnerabilidad frente a cambios de fase, pues al proteger los estados |0> y |1> codificamos $(1/\sqrt{2})(|0> \pm |1>)$ como $(1/\sqrt{2})(|000> \pm |111>)$, donde un cambio de fase en cualquier qubit estropea la combinación y, al haber más qubits, es más fácil

que el fallo se produzca. Un código cuántico de detección de errores (en adelante QECC) debe proteger el subespacio completo que contiene la información. Si observamos el comportamiento del operador de Hadamard , encontramos el hecho de que la información puede estar contenida tanto en los bits como en las fases, y que se puede pasar de una representación a otra. La aplicación de la transformación de Hadamard convierte los errores de bit en errores de fase y los de fase en errores de bit. Apliquemos esta transformación a los estados de la base ecuación 50. El resultado:

$$|0>\rightarrow \frac{1}{2}(|000>+|011>+|101>+|110>)$$

$$|1>\rightarrow \frac{1}{2}(|111>+|100>+|010>+|001>)$$

Ahora la protección contra errores de bit se ha convertido en protección contra errores de fase. Un error de fase en el tercer qubit, por ejemplo, lleva a un estado ortogonal

$$\frac{1}{2}(|000>+|011>+|101>+|110>)$$

A los de la base, y al salirse de ella el error se hace fácilmente identificable. Como era de esperar, al aplicar la transformación de Hadamard para hacer más seguro el código ante errores de fase, perdemos de nuevo la seguridad ante errores de bit. Esto se ve claramente si tenemos en cuenta que un error en cualquier qubit de una de las dos palabras lleva a la otra. Si no nos salimos de las palabras del código no tenemos forma de saber si se ha producido un error.

Pero no todos los cambios de fase son inversiones

En general un error de fase se representa por la aplicación del operador:

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Las inversiones de fase son desde luego un caso particular de este tipo de errores, donde $\theta = \pi$. En la construcción anterior sólo hemos considerado inversiones de fase, de modo que da la impresión de que prácticamente no hemos hecho nada. Sin embargo ocurre que el código anterior no sólo protege contra inversiones de fase, sino también contra todos los errores de fase.

Cualquier estado cuántico puede variar en un factor de fase global sin perder su contenido informativo. Esto nos permite escribir el error de fase como:

$$\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix}; \phi = \frac{-\phi}{2}$$

Para darnos cuenta de que tal cosa es posible consideremos este error actuando sobre el primer bit del estado |0> codificado:

$$|0> \rightarrow e^{i\phi}(|000> + |011> + e^{-i\phi}|101> + |110>) =$$
$$= \cos\phi(|000> + |011> + |101> + |110>) +$$
$$+ \sin\phi(|000> + |011> - |101> + |110>)$$

Lo que aparece tras la ocurrencia del error es la superposición del estado |0> codificado sin errores con amplitud de probabilidad $\cos\phi$, y de un estado codificado con un error de fase en el primer bit, cuya amplitud de probabilidad es $\sin\phi$. Al hacer la medida del estado resultante encontraremos el estado sin errores con probabilidad $\cos^2\phi$ y el estado con

error con probabilidad $\sin^2\phi$. La medida provoca el colapso de la función de onda, de modo que si encontramos la medida errónea sabremos cómo corregir el error en el estado del sistema. Esto prueba que cualquier error de fase es corregible con la técnica anteriormente descrita.

3.3 Previniendo errores de fase y de bit al mismo tiempo.

Una vez que conocemos una estrategia para evitar tanto un tipo de error como otro, nos interesa el modo de evitar ambos a la vez. Para hacerlo, combinaremos ambas técnicas, triplicando el número de qubits. El siguiente código deja clara la idea:

$$|0> \rightarrow \frac{1}{2}(|000> + |011> + |101> + |110>) \rightarrow$$

$$\rightarrow \frac{1}{2}(|000000000> + |000111111> + |111000111> + |111111000>)$$

$$|1> \rightarrow \frac{1}{2}(|111> + |100> + |010> + |001>) \rightarrow$$

$$\rightarrow \frac{1}{2}(|111111111> + |111000000> + |000111000> + |000000111>)$$

Obsérvese que lo único que diferencia el código definitivo del intermedio es la triplicación de cada qubit. La redundancia proteje contra los errores de bit, mientras que la etapa anterior (redundancia procesada con el operador de Hadamard) evita los errores de fase. Las técnicas empleadas no interfieren entre sí: por ejemplo, un error de bit es corregido vía chequeo de la redundancia sin afectar con ello a la fase de la superposición.

3.4 ¿Que otros errores no hemos tenido en cuenta?

No sólo hay errores de fase y de bit, de hecho hay un espacio de errores completo. De los infinitos errores posibles sólo hemos visto dos posibilidades. Afortunadamente, siendo capaces de corregir cualquier error

de bit o de fase podremos corregir también todos los demás tipos de errores. La matriz identidad y las matrices de Pauli

$$\sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Forman un espacio para todas las matrices de 4X4. La matriz identidad no hace falta decir que corresponde a la ausencia de error. No hacía falta, pero lo acabo de decir. La matriz σ_x corresponde a una inversión de bit, la matriz σ_z corresponde a un error de fase y σ_y representa una combinación de ambos errores. Como podemos corregir los diferentes errores asociados a las matrices de Pauli, y cualquier otro error es resultado de combinarlas, podemos corregir toda clase de errores. Encontramos que si podemos corregir cualquier producto tensorial de k matrices actuando sobre qubits diferentes entonces podemos corregir cualquier error que se produzca sobre k qubits.

Cuando realizamos la codificación estamos separando el espacio de los estados con la información del de los posibles errores en dimensiones ortogonales del espacio de Hilbert. La ventaja de esto es que al hacer un chequeo para comprobar la presencia de errores no alteramos la parte del vector de estado que contiene la información, con lo que aún nos será posible corregirlos. Existen otros códigos detectores de error, como por ejemplo el de Steane, que utiliza siete qubits en lugar de nueve. Realmente hay infinitos códigos posibles. Buscando el espacio de los códigos posibles apareció un código de cinco qubits.

3.5 Otros problemas: la interconexión

El problema al que me refiero aquí hasta ahora no ha sido tenido en cuenta, pero era inevitable que apareciese. El dominio de la mecánica cuántica es un mundo a escala nanométrica, mientras que el de los usuarios

de un hipotético QC es macroscópico. Es de suponer que para explotar las ventajas de la mecánica cuántica no escalaremos dispositivos tales como los cables que salgan fuera del procesador, ni, desde luego la interfaces con nosotros mismos, pues no hemos previsto encoger. Así que nos encontramos con un procesador de información constituida a partir de elementos de escala nanométrica, y tiempos de respuesta característicos de los sistemas cuánticos conectado a unos hipotéticos detectores y electrodos de control que deben ser capaces por un lado de controlar individualmente las entradas y medir las salidas, y por otro asociarse de modo que puedan funcionar coordinados para, por ejemplo, la medida del estado de un registro cuántico, tal vez constituida por miles de qubits, y llevar información de un dominio a otro sin cometer errores. Todo esto teniendo en cuenta que a escala macroscópica los tiempos característicos son siempre órdenes de magnitud mayores.

3.6 Alternativas para la construcción del computador cuántico

Una vez llegados a este punto es momento de comenzar a hablar sobre como construir computadores cuánticos, tanto de qué se ha hecho como de que se considera hacer en el futuro. El tema abandona la teoría de la información, para ocuparse de aspectos más convencionales; podríamos decir que se trata de ingeniería. Esto nos limita desde la perspectiva de que no basta con encontrar un modo de fabricar un QC, sino que además esto debe conseguirse dentro de costes que se consideren aceptables. También puede significar que en la práctica se escoja una alternativa de fabricación en lugar de otra más eficiente por motivos relacionados con los medios de producción, etc.. Sin embargo, la búsqueda de sistemas físicos capaces de servirnos supone la necesidad de resolver el problema de la evolución de sistemas cuánticos determinados, y en ese sentido estamos haciendo física.

A nivel elemental tenemos bastante idea sobre cómo realizar distintas operaciones sobre qubits. Desde luego, tal cosa depende de cómo hayamos escogido implementar los qubits en el QC. Cualquier transición entre niveles

energéticos que fuéramos capaces de estimular podría ser un modo de actuar sobre los qubits, si es que hemos decidido almacenarlos de esta manera.

Nos enfrentamos a una de las mayores dificultades en la construcción del QC: la escala. Un procesador cuántico de la información debe ser controlable, de modo que podamos realizar controladamente operaciones sobre los qubits, de acuerdo a la definición de la sección El computador Cuantico, pero al mismo tiempo debe ser lo bastante grande como para que sea útil. En la sección Factorizacion de Enteros Grandes se dijo que un QC no aporta ninguna ventaja sobre un computador convencional al factorizar números de 130 dígitos o menos.

El reto consiste en descubrir que sistemas físicos podemos emplear para realizar cálculos, que cumplan los requisitos anteriores. Lo primero que se nos viene a la cabeza es tratar de fabricar procesadores de estado sólido, del mismo modo que en computación clásica, pero tropezamos con la decoherencia. En el interior de un sólido el acoplamiento entre vecinos es fuerte, de modo que cualquier estado que consiguiésemos producir se perdería en tiempos del orden de picosegundos. En concreto, donde la decoherencia actúa tan deprisa en en la destrucción de la fase de las superposiciones de estados, que son la clave para conseguir por ejemplo que la factorización se realice tan deprisa.

Dos de las alternativas posibles parece que pueden utilizarse para manejar decenas de qubits: se trata de las trampas iónicas (propuestas por Zirac y Zoller en 1995), y la de aprovechar la ``bulk'' resonancia magnética (de Gershenfeld y Chuang en 1997 y Cory et. al. en 1996) de las cuales hablaremos adelante.

3.6.1 Computadores Cuánticos.

Que es un computador cuantico según David Deutch[3] (1985,1989), "Un computador cuantico es una colección de n qubits sobre los cuales es posible:

1. Cada qubit puede prepararse en un estado conocido |0>
2. Los qubits pueden medirse en la base {|0>,|1>}
3. Sobre cualquier subconjunto de qubits de tamaño fijo podemos aplicar na (o un conjunto de) puertas universales.
4. Los qubits sólo evolucionarán de la manera prevista en las puertas.

El último punto es el que trae más problemas, debido a la existencia de decoherencia. No podemos esperar de un sistema cuántico convencional que su evolución se produzca de manera totalmente controlada. Si bien esta es una limitación física, podríamos modificar el enunciado de modo que fuese menos restrictivo, al tiempo que lo suficiente para poder seguir llevándonos a una definición útil. Por ejemplo, podríamos conformarnos con un sistema cuya evolución fuese al menos en cierta medida controlada, de modo que una parte de la información que contiene evolucionase de un modo previsible."

3.6.2 Modelos de computador.

La discusión sobre modelos particulares de computador está aquí orientada hacia la construcción, pero no desde el punto de vista físico, si no de diseño.

El modelo de circuito cuántico.

El modelo de red es el más utilizado en computación convencional. Se basa, en la concatenación de etapas de puertas lógicas (no

[3] David Deutch: Cientifico aleman que escribio muchos libros de Computación Cuantica como Opening Paragraphs of The Fabric of Reality.

necesariamente binarias). Este modelo es fácilmente traducible a un mundo de puertas lógicas cuánticas, si bien no aporta nada nuevo sobre el modelo tradicional, y tropieza con muchas dificultades. La ventaja que tiene no es otra que el hecho de ser un modelo más maduro, y por tanto con más posibilidades de llevarse al laboratorio. El inconveniente consiste en que lo que hacemos es trasladar un diseño que surgió para sistemas clásicos al campo de los sistemas cuánticos, por lo que el modelo en sí no explota las particularidades de este dominio.

Aquí no debemos entender las puertas lógicas como en los circuitos electrónicos. En un circuito electrónico un a puerta lógica era algún dispositivo físico que encuentra una señal eléctrica a su paso, y que es capaz de permitirle o no el paso en función de unas determinadas circunstancias.

En una red cuántica, en cambio, las puertas lógicas no pueden realizarse de esta manera por varias razones. Entre otras cosas, no podemos clonar a voluntad un cierto estado, mientras que en un circito electrónico esto es inmediato. Por otra parte, la naturaleza de los qubits (habitualmente magnética) requiere que utilicemos por ejemplo campos magnéticos para manipularlos.

Podemos entonces preparar una especie de trayectoria que vaya recorriendo todo el sistema, salpicada de regiones donde producimos campos magnéticos durante tiempos tan cortos que podamos estar seguros de que sólo afectan a un qubit, y tan bien sincronizados que además sabremos a que qubit afectan. Deberíamos hacer tantos de estos dispositivos como etapas tenga la operación que hayamos previsto realizar. Todo esto resulta absurdamente complicado.

Lo razonable es dejar los qubits fijos en el espacio, y operar sobre ellos con un único conjunto de actuadores que produzcan los respectivos campos magnéticos, o el efecto que queramos aprovechar para modificar el estado

del arreglo. Si se tratara de campos magnéticos, obligando a los spines a orientarse de determinada manera, no sería necesario que nos preocupáramos de si éstos están activos un poco más de tiempo de la cuenta, pues cada electrón acabaría en el mismo estado final. Así tenemos que la idea de red en computación cuántica tiene muy poco que ver con la de la computación tradicional.

3.6.3 El autómata celular cuántico (QCA).

A diferencia de los modelos anteriores, el autómata celular cuántico está diseñado de modo que aprovecha el comportamiento de los sistemas a escala cuántica. El modelo de red o circuito cuántico, por ejemplo, no trata de ser más que una adaptación del modelo de circuito tradicional, aunque como tal tropieza con dificultades, como la imposibilidad de clonar los estados y el hecho de que debemos pensar en las operaciones como operadores actuando sobre registros cuánticos, y no necesariamente como etapas en la propagación de señales. Se Hablara en detalle sobre este modelo pues de mucho interés.

3.7 Construcción del computador cuántico.

Por ahora no hablamos de computadores cuánticos, sino de procesadores cuánticos de la información, siendo incluso esta denominación pretenciosa. Al hablar de computador cuántico nos referimos a una máquina de propósito general, capaz de ejecutar cualquier tarea simplemente preparándola de modo adecuado. Un procesador de información puede ser una máquina con una tarea mucho más específica, tal como realizar operaciones matemáticas, o adaptar señales eléctricas para digitalizar sonidos. Las tareas que la mecánica cuántica computa de manera más eficiente que la clásica no son todas; de hecho, son una pequeña parte, cuya aplicabilidad en el fondo es más bien reducida. Un usuario corriente no está preocupado de simular sistemas físicos ni de romper claves seguras en las comunicaciones de otros usuarios. De hecho, la mayoría tampoco aspiran a

utilizar criptografía cuántica en sus mensajes, dado que en ellos no hay un contenido cuya protección merezca inversiones económicas tan fuertes.

Vistas las cosas de este modo parece que, al menos como primer fin, el objetivo a nivel tecnológico en computación cuántica es el de construir máquinas capaces de ejecutar específicamente aquellas tareas en las que la mecánica cuántica suponga una verdadera ventaja, independientemente del coste, dado que los primeros usuarios serán instituciones públicas o grandes compañías. Algo parecido ocurrió con la computación electrónica, aunque su evolución desembocó finalmente en la situación que conocemos hoy en día.

3.7.1 Trampas iónicas.

La descripción de un procesador que se aprovecha de trampas iónicas puede hacerse del siguiente modo:

Disponemos de una ``Trampa de Paul'', que en esencia es una región de alto vacío (hablamos del orden de 10^{-8} Pa), donde una cadena de iones se mantiene confinada utilizando una combinación de campos eléctricos oscilantes y estáticos.

Hay un haz láser que se desdobla por medio de desdobladores de haces y moduladores acustoópticos. Obtenemos por este medio un par de haces para cada ión.

Cada ión tiene dos estados de vida media lo más larga posible. Podemos usar los sub-niveles de estructura fina del nivel fundamental. Llamaremos a los estados correspondientes |g> y |e>. Dado que van asociados a energías diferentes (en la base de estados de estructura hiperfina es donde podemos distinguirlos), son necesariamente ortogonales.

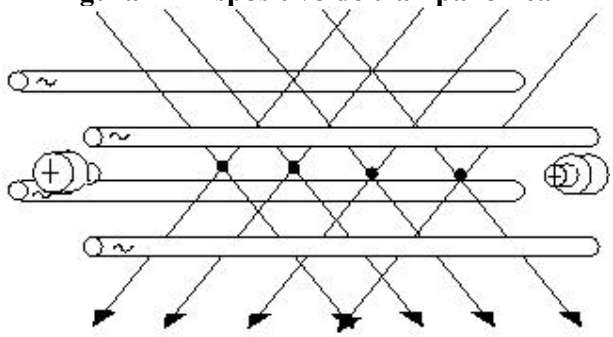
Los pares de hacer láser se utilizan para inducir transiciones Ramman coherentes entre los niveles en los que hemos codificado los qubits. Esto

permite aplicar operaciones sobre cada qubit, pero no operaciones sobre más de uno, tales como las puertas binarias o ternarias.

Para realizar operaciones sobre más de un qubit, tales como las binarias, aprovecharemos la repulsión culombiana entre los iones. Para hacerlo utilizamos un resultado de Zirac y Zoller que analizaremos a continuación.

La siguiente figura muestra un esquema del dispositivo:

Figura 17 Dispositivo de trampa ionica



Los haces de fotones que utilizamos para modificar el estado de los iones además de energía transportan momento. El momento suministrado a los iones se traduce en que toda la cadena se mantiene en estados vibracionales globales, que naturalmente se encuentran cuantizados, puesto que la trampa iónica mantiene confinados a los iones. Esto se conoce como efecto Mössbauer. Los estados de la cadena corresponden a números enteros de cuantos de energía de vibración, precisamente fotones.

El nivel fundamental de vibración corresponderá al estado |n=0>, mientras que el primer nivel excitado lo hará con |n=1>, y así sucesivamente.

Supongamos que queremos realizar la operación Z controlada. Para realizar esta operación entre los iones x_i y x_j desde el estado vibracional

fundamental |n=0>, hacemos que una pareja de haces de fotones lleven a cabo sobre el ión x_i la transición:

$$|n=0>|g>_i \rightarrow |n>=|n=0>|g>_i$$

$$|n=0>|e>_i \rightarrow |n>=1>|g>_i$$

De modo que x_i siempre acaba en el estado interno fundamental. El estado de movimiento del i-ésimo ión queda así inicializado. A continuación aplicamos una pareja de haces sobre x_j de modo que se produzca la transición:

$$|n=0>|g>_j \rightarrow |n=0>|g>_j$$

$$|n=0>|e>_j \rightarrow |n=0>|e>_j$$

$$|n=1>|g>_j \rightarrow |n=1>|g>_j$$

$$|n=1>|e>_j \rightarrow -|n=1>|e>_j$$

Esto es, invertir el estado de x_i sólo cuando nos encontremos al ión en el primer estado vibracional y en el nivel interno |e>.

Ahora aplicaremos de nuevo el puso inicial sobre x_i. El efecto de los tres pulsos se resume en:

$$|n=0>|g>_i|g>_j \rightarrow |n=0>|g>_i|g>_j$$

$$|n=0>|g>_i|e>_j \rightarrow |n=0>|g>_i|e>_j$$

$$|n=0>|e>_i|g>_j \rightarrow |n=0>|e>_i|g>_j$$

$$|n=0>|e>_i|e>_j \rightarrow -|n=0>|e>_i|e>_j$$

Donde hemos actuado solamente sobre los estados internos de los iones, aunque para hacerlo nos hayamos aprovechado de los estados vibracionales.

La puerta Z controlada, junto con las transformaciones sobre un único qubit también constituye un conjunto de primitivas de la computación cuántica, análogamente al descrito en la sección de Puertas cuanticas.

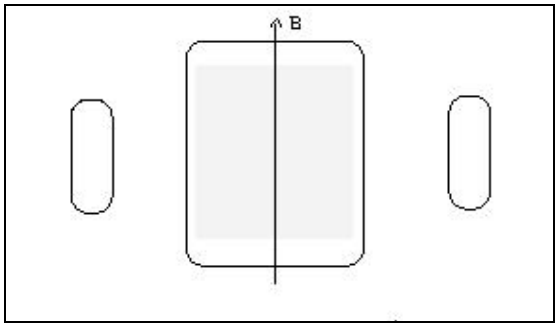
Recordemos (El computador Cuantico) que también debemos ser capaces de preparar la cadena en el estado |000...>, y que debemos ser capaces de medir el estado final. La primera operación la realizaremos por medio de bombeo óptico y enfriamiento láser, mientras que la medida puede hacerse con técnicas como el salto cuántico y el shelving electrónico.

Para llevar los iones al nivel energético más bajo de estructura hiperfina hace falta llevar la temperatura por debajo de la millonésima de grado Kelvin. La principal fuente de decoherencia aquí es el calentamiento debido a la interacción entre el movimiento de la cadena y el ruido en los electrodos. Aún no se sabe como evitar este problema.

3.7.2 Resonancia magnética nuclear.

La siguiente propuesta se esquematiza en esta figura:

Figura 18 Procesados por Resonancia Magnética Nuclear (RMN)



.

En el interior de la cápsula tenemos moléculas con un esqueleto interno de alrededor de 10 átomos, fijados a algunos otros por enlaces químicos. Para los núcleos de estas moléculas hay un momento magnético asociado a su spin nuclear. Estos spines serán los que utilizaremos como qbits. Las moléculas de este tipo son sometidas a un elevado campo magnético, y sus estados son manipulados por medio de pulsos magnéticos de duración controlada.

El problema en esta situación es que no hay modo de preparar una molécula en un estado inicial determinado. Entonces, en lugar de una única molécula, utilizamos un fluido con alrededor de 10^{20} moléculas, y medimos el spin promedio, cosa que puede hacerse si el momento magnético de los núcleos es lo bastante elevado como para producir un efecto medible.

El campo magnético no tiene el mismo valor en todos los puntos del recipiente, de modo que la evolución de cada procesador molecular es ligeramente diferente. Aplicamos entonces una técnica llamada de spin-echo, lo que permite invertir el efecto de la evolución libre de cada spin, sin que el efecto de las puertas cuánticas desecho. El pago por hacerlo es el aumento de la dificultad de implementación de muchas operaciones seguidas.

Volvamos al problema de la preparación del estado inicial. El líquido con el que operaremos se encuentra en equilibrio térmico, de modo que las probabilidades de ocupación de los distintos estados de spin obedecen a la distribución de Boltzmann. Además, partimos de la base de que las energías de estos estados son muy parecidas, con lo que las probabilidades de ocupación lo serán también. La matriz densidad de alrededor de 10^{20} spines nucleares se parece mucho a la matriz identidad.

$$\Delta = \rho - I$$

La matriz Δ(la pequeña diferencia) es la que se utiliza para almacenar la información. Esta no es la matriz densidad, pero se transforma del mismo modo que ella bajo pulsos magnéticos adecuadamente escogidos. De este modo, podemos llamar a este sistema un computador cuántico efectivo.

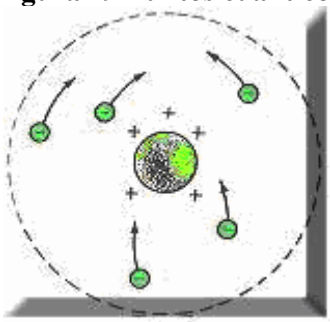
Actualmente somos capaces de manipular experimentalmente una cantidad de spines suficientemente elevada como para realizar operaciones con unos pocos qubits. Esto hace pensar que los primeros procesadores de información cuánticos aprovecharán esta técnica.

Lo malo es que no podemos aumentar indefinidamente la escala de computación esperando un comportamiento igualmente bueno. Con n qubits la señal pierde potencia en un factor 2^{-n}, de modo que no podemos aumentar indefinidamente el número de qubits. Otro problema que aparece es que al poder manejar solamente estados promedio de los spines nos vemos limitados para aplicar técnicas de corrección de errores.

3.7.3 Quantum dots

Que son los Quantum Dots

Figura 19 Puntos cuanticos



Consiste básicamente en un electrón atrapado dentro de un conjunto de átomos (jaula de átomos), el cual, mediante un rayo láser de una frecuencia específica, se traslada de su estado no excitado ("cero") a su

estado excitado ("uno") y viceversa. Si la duración de la exposición al láser es igual a la mitad del tiempo requerido para cambiar el nivel energético del electrón, este adquiere un estado de superposición de sus dos valores posibles.

A continuación se explorara otra posibilidad para la construcción del QC, spines electrónicos en puntos cuánticos. Además de puntos cuánticos podríamos hacer uso de otros medios de confinamiento, tales como átomos o moléculas. Sin embargo, dado el grado de desarrollo de las técnicas experimentales asociadas a los quantum dots parece que esta será una de las primeras formas en que veremos construir a los computadores cuánticos.

Los puntos cuánticos también se denominan átomos artificiales, debido a que son capaces de mantener electrones estados ligados, del mismo modo que los átomos... pero son mucho más fáciles de controlar. Los dispositivos de este tipo sabemos que permiten incrementar el número de qubits, y que la decoherencia no es tan importante como en otros esquemas.

En estructuras de Gas podemos hacer variar el número de qubits de uno en uno. Longitudes magnéticas del orden de 1nm se obtienen con campos de 1T, y esa es la escala de los quantum dots. Con quantum dots acoplados observamos efectos como la formación de un estado deslocalizado, ``molecular''. El entrelazamiento nos va a permitir realizar las operaciones que describí antes.

Elegimos entonces a los spines electrónicos como nuestros qubits, y a los quantum dots como los responsables del confinamiento. Ahora necesitamos una fuente de entrelazamiento que sea determista. Dicho de otro modo, un modo de hacer que los qubits interactúen entre ellos (por ejmplo, a través de una XOR). Dos sistemas aislados no podrán nunca influir

el uno sobre el otro. Podemos acoplar los spines durante un tiempo para conseguir esta interacción. Si tenemos en cuenta por lado la repulsión de Coulomb y por otro el principio de exclusión de Pauli, llegaremos a que el estado fundamental de una pareja de electrones acoplados es un singlete, que desde luego tiene un elevado grado de entrelazamiento.

Estamos interesados en la realización de las operaciones sobre los qubits, y a la luz de lo que acabamos de ver parece buena idea estudiar el hamiltoniano de acoplamiento. El hecho de tratarse de un singlete conlleva una energía de canje, asociada a la interacción entre spines:

$$H_s = J(t)s_1.s_2$$

Supongamos que hacemos actuar a la energía de intercambio, de modo que tengamos:

$$\frac{1}{h}\int J(t)dt = \frac{Jo\,\tau_s}{h} = (2n+1)\pi, n = 0,1....$$

Entonces la evolución del sistema vendrá dada por el operador unitario:

$$U(t) = T\left(e^{\frac{i}{h}\int_0^t H_s(\tau)d\tau}\right)$$

Esta evolución corresponde al operador de intercambio, Usw, que intercambia ambos electrones. Lo interesante está en esta igualdad:

$$Uxor = e^{\frac{i\pi}{2}S_z^1} e^{\frac{i\pi}{2}(S_Z^1 - S_Z^2)U_{sw}^{1/2}}$$

Aquí hay dos operaciones diferentes, $U_{sw}^{1/2}$, donde U_{sw} es el operador de intercambio, y una rotación de un único qubit, $e^{I\pi S_z^1}$.

El resultado, nada menos que la aplicación de una puerta XOR. El estudio de la implementación de funciones con qubits, bajo este esquema (y otros parecidos) se reduce entonces al del mecanismo de acoplamiento J(t), y de su control externo.

4 LA COMPUTACIÓN CUÁNTICA EN LA CRIPTOGRAFÍA

4.1 Conceptos de Criptografía

Introducción

La criptografía cuántica es una nueva área dentro de la criptografía que hace uso de los principios de la física cuántica para transmitir información de forma tal que solo pueda ser accedida por el destinatario previsto.

Para poder llegar a explicar los detalles de la criptografía cuántica se necesitan establecer algunos conceptos básicos de criptografía y física cuántica que serán de ayuda para la comprensión del tema. Pero antes que nada se expone el problema que la criptografía cuántica intentará solucionar.

El Problema de Alice y Bob

A continuación se plantea un problema del cual participan dos caracteres principales, **Alice** y **Bob**. Alice desea comunicarse con Bob, pero como no se encuentran en el mismo lugar, lo hará a través de algún tipo de enlace.

El problema en cuestión se presenta con la aparición de un tercer personaje al que llamaremos **Eve**, quien intentará escuchar la comunicación entre Alice y Bob quienes al mismo tiempo no desean ser escuchados.

Figura 20 Envío de mensajes

La criptografía presenta varios métodos para evitar que si una comunicación es escuchada por terceras personas, éstas puedan comprender su contenido.

La criptografía cuántica provee una contribución única al campo de la criptografía. La criptografía cuántica provee un mecanismo que permite a las partes que se están comunicando entre si a:

Detectar Automáticamente Escuchas

En consecuencia, proporciona un medio para determinar cuando una comunicación encriptada ha sido comprometida, es decir si se está efectuando una escucha secreta y no autorizada sobre la misma.

A partir de de este momento se hará uso de los nombres Alice, Bob y Eve para referirse respectivamente al emisor, al receptor y a quien escucha secretamente los mensajes de una comunicación.

Los nombres **A**lice y **B**ob son utilizados tradicionalmente en lugar de las letras **A** y **B** en ejemplos de comunicaciones y criptografía para hacer referencia a los participantes de una comunicación entre dos puntos. El nombre **E**ve proviene de la palabra inglesa **E**vesdropper cuya traducción es “quien escucha secretamente”.

4.2 Conceptos de Criptografía

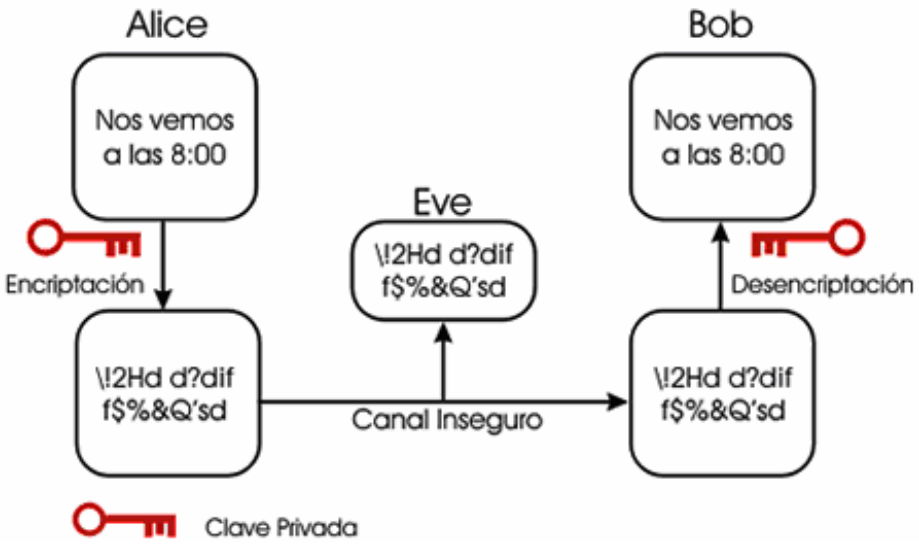
Las técnicas de encriptación se suelen dividir en dos grupos: algoritmos de clave privada y algoritmos de clave pública. A los algoritmos de clave privada se los llama también algoritmos de encriptación simétricos o convencionales mientras que a los de clave pública también se los suelen denominar algoritmos antisimétricos.

4.3 Modelo de Criptografía Convencional o de Clave Privada

En el modelo convencional, el mensaje original que es comprensible se convierte en un mensaje que aparentemente es aleatorio y sin sentido. El proceso de encriptación consta de dos partes, un algoritmo y una clave. La clave es un valor que es independiente del texto o mensaje a cifrar. El algoritmo va a producir una salida diferente para el mismo texto de entrada dependiendo de la clave utilizada.

Una vez cifrado, el mensaje puede ser transmitido. El mensaje original puede ser recuperado a través de un algoritmo de desencriptación y la clave usada para la encriptación.

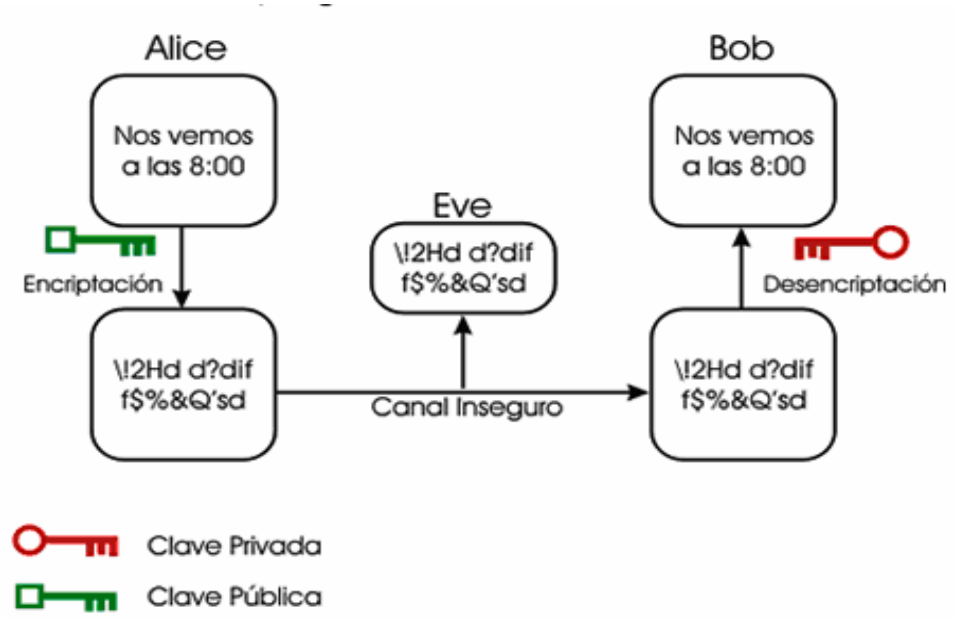
Figura 21 Criptografía de clave privada



4.3.1 Modelo de Criptografía de Clave Pública

Los algoritmos de criptografía pública se basan en una clave para encriptación y una clave relacionada pero distinta para la desencriptación. Estos algoritmos tienen la característica de que es computacionalmente imposible determinar la clave de desencriptación (clave privada) a partir del algoritmo criptográfico y la clave de encriptación (clave pública).

Figura 22 Criptografia de calve publica



Los pasos del proceso de encriptación con clave pública son los siguientes:

- Cada sistema genera un par de claves para ser usadas en la encriptación y desencriptación de los mensajes que envíen y reciban.
- Cada sistema publica su clave de encriptación (clave pública). La clave de desencriptación relacionada (clave privada) se mantiene en privado.
- Si Alice desea enviar un mensaje a Bob, encripta el mensaje utilizando la clave pública de Bob.

- Cuando Bob recibe un mensaje lo desencripta usando su clave privada. Nadie puede desencriptar el mensaje porque solo Bob conoce su clave privada.

4.3.2 Criptosistema Caesar

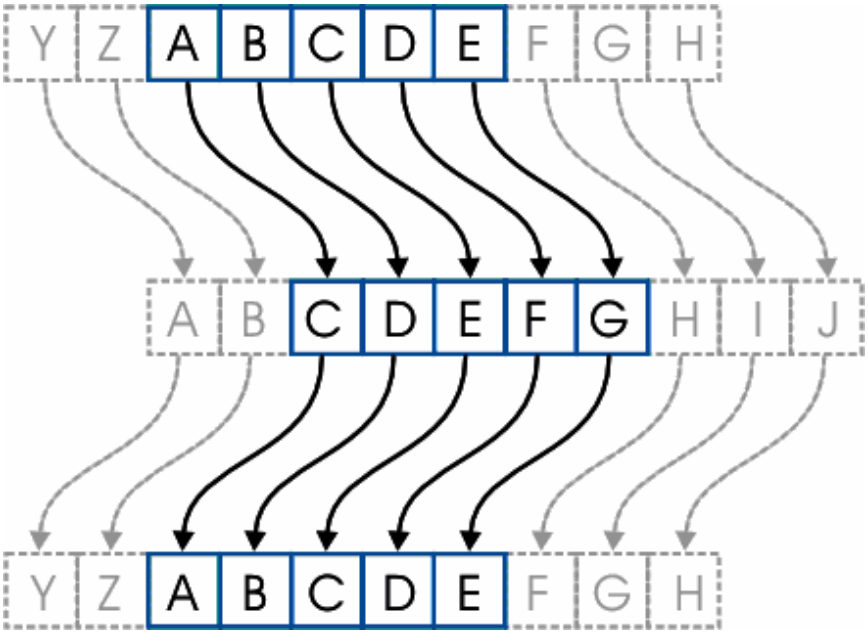
El sistema Caesar o desplazamientos Caesar es una de las tecnicas de criptografía más simples y mayormente difundidas. Fue el primero que se utilizó del cual se tienen registros. El sistema es monoalfabético y es realmente muy malo, su único valor es el valor histórico de haber sido el primero.

En un sistema Caesar la encriptación se hace por sustitución, cada caracter del mensaje original será reemplazado por un caracter en el mensaje cifrado, el caracter cifrado se obtiene avanzando 'k' pasos en el alfabeto a partir del caracter original. Obviamente 'k' es la clave.

Ejemplo con **k=2**:

Si el texto original es "ABCDE" se codifica como "CDEFG"

Figura 23 Método criptografico CAESAR



Este es todo el secreto del sistema 'CAESAR' veamos ahora cuan malo es:

Criptoanálisis

Para el sistema Caesar la tarea de un criptoanalista es realmente sencilla, pues la cantidad de posibles claves de este sistema es muy limitada. Trabajando con un alfabeto de 25 caracteres hay solamente 25 posibles claves (1..25) la clave 26, es idéntica a la clave 1, la clave 27 es idéntica a la 2 y así sucesivamente. De esta forma el criptoanalista puede chequear una por una las 25 posibles claves y observando el resultado obtenido se llega fácilmente y en muy poco tiempo al mensaje original.

Este es un criptosistema cuyo punto débil es el espacio de claves, como hay muy pocas claves posibles la técnica mas recomendable para el criptoanalista es simplemente probar todas las posibles claves. A este método se lo denomina 'ataque por fuerza bruta' y cuando el tiempo estimado para el ataque es razonable es un método infalible.

4.3.3 Criptosistema DES

Finalmente analizaremos el sistema de encriptación por clave privada mas difundido y ampliamente utilizado en el mundo conocido como 'DES' (Data Encription Standard) Cuando fue creado el algoritmo se suponía tan fuerte que inmediatamente se propuso como standard y se dio a conocer el algoritmo.

El Estándar Federal para encriptación de datos. (DES) fue durante mucho tiempo un buen algoritmo de encriptación para la mayoría de las aplicaciones comerciales. El gobierno de USA, sin embargo nunca confío en el DES para proteger sus datos clasificados debido a que la longitud de la clave del DES era de solamente 56 bits, lo suficientemente corta como para ser vulnerable a un ataque por fuerza bruta.

El ataque mas devastador contra el DES fue descripto en la conferencia Crypto'93 donde Michael Wiener de Bell presento un trabajo sobre como crackear el DES con una maquina especial. El diseño consistía en un Chip especial que probaba 50 millones de claves DES por segundo hasta que encontraba la correcta, estos chips podían producirse por $10.50 cada uno, y Wiener había desarrollado una maquina especial que reunía 57000 de estos chips a un costo de un millón de dólares. La maquina era capaz de crackear cualquier clave DES en menos de siete horas promediando 3.5 horas por clave. Por 10 millones Wiener construía una maquina que tardaba 21 minutos por clave. Y por 100 millones el tiempo se reducía a dos minutos por clave. Desde ese momento el DES de 56 bits no volvió a ser utilizado con propósitos serios de encriptación de datos.

Un posible sucesor del DES es una versión conocida como Triple-DES que usa dos claves DES para encriptar tres veces, alcanzando un rendimiento equivalente a una única clave de 112 bits, obviamente este nuevo esquema es tres veces mas lento que el DES común.

El algoritmo que sucedió al DES y que es actualmente utilizado por el PGP entre otros es el IDEA (International data encription algorithm).

IDEA usa claves de 128 bits y esta basado en el concepto de "mezclar operaciones de distintos grupos algebraicos" (?!) Es mucho mas rápido en sus implementaciones que el DES. Al igual que el DES puede ser usado como cipher-feedback (CFB) o cipher-block-chaining (CBC). EL PGP lo utiliza en modo CFB de 64 bits.

El algoritmo IPES/IDEA fue desarrollado en ETH Zurich por James Massey y Xuejia Lai y publicado por primera vez en 1990. IDEA ha resistido ataques mucho mejor que otros cifradores como FEAL,REDOC-II,LOKI,Snefru y Khafre. Biham y Shamir han sometido al algoritmo IDEA a técnicas de criptoanálisis sin encontrar hasta el momento debilidad alguna en el algoritmo. Grupos de criptoanálisis de varios países se encuentran abocados a atacar el algoritmo para verificar su confiabilidad.

4.3.4 Criptosistema Hill

Este sistema esta basado en el álgebra lineal y ha sido importante en la historia de la criptografía. Fue Inventado por Lester S. Hill en 1929, y fue el primer sistema criptografico polialfabético que era práctico para trabajar con mas de tres símbolos simultaneamente.

Este sistema es polialfabético pues puede darse que un mismo caracter en un mensaje a enviar se encripte en dos caracteres distintos en el mensaje encriptado.

Suponiendo que trabajamos con un alfabeto de 26 caracteres.

Las letras se numeran en orden alfabético de forma tal que A=0, B=1, ... ,Z=25

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Se elije un entero d que determina bloques de d elementos que son tratados como un vector de d dimensiones.

Se elije de forma aleatorea una matriz de d × d elementos los cuales seran la clave a utilizar. Los elementos de la matriz de d × d serán enteros entre 0 y 25, además la matriz M debe ser inversible en $\mathbb{Z}_{26}^{n}$. Para la encriptación, el texto es dividido en bloques de d elementos los cuales se multiplican por la matriz d × d

Todas las operaciones aritméticas se realizan en la forma modulo 26, es decir que 26=0, 27=1, 28=2 etc. Dado un mensaje a encriptar debemos tomar bloques del mensaje de "d" caracteres y aplicar: $M \times P_i = C$, donde C es el código cifrado para el mensaje P_i

Ejemplo:

Si tomamos la matriz $A = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}$ como matriz de claves.

Para encriptar el mensaje "CODIGO" debemos encriptar los seis caracteres de "CODIGO" en bloques de 3 caracteres cada uno, el primer bloque

$$P_1 = "COD" \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix} \quad P2 = "IGO" \begin{pmatrix} 6 \\ 8 \\ 14 \end{pmatrix}$$

$$A.P_1 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}\begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix} = \begin{pmatrix} 308 \\ 349 \\ 197 \end{pmatrix} = \begin{pmatrix} 22 \\ 11 \\ 15 \end{pmatrix} (\text{mod } 26)$$

El primer bloque "COD" se codificara como "WLP"

$$A.P_1 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}\begin{pmatrix} 8 \\ 6 \\ 14 \end{pmatrix} = \begin{pmatrix} 422 \\ 252 \\ 264 \end{pmatrix} = \begin{pmatrix} 6 \\ 18 \\ 4 \end{pmatrix} (\text{mod } 26)$$

El segundo bloque "IGO" se codificara como "GSE"

Luego 'CODIGO' encriptado equivale a 'WLPGSE'.

Observar que las dos "O" se codificaran de forma diferente.

Para desencriptar el método es idéntico al anterior pero usando la matriz inversa de la usada para encriptar.

Cálculo de la matriz inversa

Antes que nada debemos verificar que la matriz elegida sea invertible en modulo 26. Hay una forma relativamente sencilla de averiguar esto a través del cálculo del determinante. Si el determinante de la matriz es 0 o tiene factores comunes con el módulo (en el caso de 26 los factores son 2 y 13), entonces la matriz no puede utilizarse. Al ser 2 uno de los factores de 26 muchas matrices no podrán utilizarse (no servirán todas en las que su determinante sea 0, un múltiplo de 2 o un múltiplo de 13)

Para ver si es invertible calculo el determinante de A

$$\begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}$$

5 (23 · 13 – 3 ·11) – 17 (9 · 13 – 3 · 2) + 20 (9 · 11 – 23 · 2) =

1215 – 1734 + 1060 = 503

503 = 9 mod 26

La matriz A es invertible en modulo 26 ya que 26 y 9 son co-primos. Para hallar la inversa de la matriz modulo 26, utilizamos la formula

$$A^{-1} = C^T.(\det(A))^{-1}$$

Donde CT es la matriz de cofactores de A transpuesta. Hay que tener en cuenta que $(\det(A))^{-1}$ debe realizarse en modulo 26

por lo tanto para el ejemplo la inversa de 9 (mod 26) es 3 (mod 26) ya que 9 (mod 26) · 3 (mod 26) = 27 mod 26 = 1 (mod 26)

Por lo tanto 3 es la inversa multiplicativa de 9 en modulo 26 . Para calcular C hay que calcular los cofactores de A

$$C_{11} = +\begin{pmatrix} 23 & 3 \\ 11 & 13 \end{pmatrix} \; C_{12} = -\begin{pmatrix} 9 & 3 \\ 2 & 13 \end{pmatrix} \; C_{13} = +\begin{pmatrix} 23 & 23 \\ 2 & 11 \end{pmatrix}$$

$$C_{21} = -\begin{pmatrix} 17 & 20 \\ 11 & 13 \end{pmatrix} \; C_{22} = +\begin{pmatrix} 5 & 20 \\ 2 & 13 \end{pmatrix} \; C_{23} = -\begin{pmatrix} 5 & 17 \\ 2 & 11 \end{pmatrix}$$

$$C_{31} = +\begin{pmatrix} 17 & 20 \\ 23 & 3 \end{pmatrix} \; C23 = -\begin{pmatrix} 5 & 20 \\ 9 & 3 \end{pmatrix} \; C_{11} = +\begin{pmatrix} 5 & 17 \\ 9 & 23 \end{pmatrix}$$

$$C = \begin{pmatrix} 266 & -111 & 53 \\ -1 & 25 & -21 \\ -409 & 168 & -38 \end{pmatrix} \; C^{\tau} = \begin{pmatrix} 266 & -1 & -409 \\ -111 & 25 & 165 \\ 53 & -21 & -38 \end{pmatrix}$$

Ahora aplicamos la formula de la inversa

$$A^{-1} = C^{t}.(\det(\ a\ ))^{-1} = \begin{pmatrix} 266 & -1 & -409 \\ -111 & 25 & -165 \\ 53 & -21 & -38 \end{pmatrix}.3$$

$$A^{-1} = \begin{pmatrix} 798 & -3 & -1227 \\ -333 & 75 & 495 \\ 159 & -63 & -114 \end{pmatrix} \quad A^{-1} = \begin{pmatrix} 18 & 23 & 21 \\ 5 & 23 & 1 \\ 3 & 15 & 16 \end{pmatrix} \bmod(\ 26\ )$$

Esta última es la matriz que utilizamos para desencriptar

Criptoanálisis

El sistema de Hill plantea a los criptoanalistas problemas mucho mayores a los que planteaba 'CAESAR'. Para empezar el espacio de claves es mucho mayor, en este caso es de 4C25, es decir las permutaciones de 4 elementos tomados de entre 25 posibles. Y usando una matriz mas grande la cantidad de posibles claves se puede hacer tan grande como sea necesario para hacer que sea imposible un ataque por fuerza bruta.

Lo mejor que puede hacer un criptoanalista es tratar de conseguir un código para el cual se conozca una parte del mensaje. Y ver si con ambos datos es capaz de encontrar cual fue la matriz utilizada para encriptar el mensaje.

4.4 Sistemas de clave pública

Los sistemas de encriptación de datos por clave publica han revolucionado el mundo de la criptografía y se han impuesto ampliamente en el mercado de las comunicaciones, la idea aunque sencilla recién surgió en la década del '70, los expertos en criptografía no logran ponerse de acuerdo

en cual fue el motivo que demorara tanto el surgimiento de este tipo de sistema de encriptación.

La idea de los sistemas de clave pública es sencilla: cada usuario genera 2 (dos) claves: una publica y una privada, el usuario debe conservar su clave privada a salvo mientras que la clave pública es distribuida en forma masiva.

El juego de claves funciona de la siguiente forma: los mensajes que son encriptados con la clave pública de un usuario solo pueden ser desencriptados con la clave privada del mismo.

El algoritmo de encriptación es publico, de forma tal que cualquiera pueda encriptar un mensaje, el algoritmo de desencriptación debe de forma tal que sin la clave privada sea muy difícil desencriptar el código mientras que con la clave privada esto es una tarea sencilla. Todos los algoritmos de encriptación por clave pública se basan en algún problema en general de tipo matemático de cuyo tiempo de resolución no pueda establecerse una cota inferior.

4.4.1 RSA

El algoritmo de clave publica más probado y utilizado en todo el mundo es el algoritmo RSA, denominado así debido a sus autores: Rivest, Shamir y Adleman.

Está basado en una idea asombrosamente sencilla de la teoría de números y hasta la fecha ha resistido todo tipo de ataques criptoanalíticos.

La idea es simple: dados dos números primos p y q muy grandes es sencillo a partir de p y q hallar su producto (p*q) pero es un problema muy complejo a partir del producto hallar los números p y q en cuestión. Si bien hasta el momento no se ha podido demostrar que la factorización prima de

un numero es un problema NP-complejo, todos los intentos realizados para factorizar un número en forma veloz han fracasado.

Sean dos números p y q primos de aproximadamente 100 dígitos cada uno.

n = p*q y §(n) = (p-1) * (q-1)

Además se elige un número random d de muchos dígitos tal que d y §(n) son relativamente primos. Y un número e, 1<e<§(n) tal que e*d=1 usando aritmética módulo §(n).

n = módulo.

e = exponente de encriptación.

d = exponente de desencriptación.

La clave pública estará formada por n y e.

La clave privada estará formada por p,q,§(n) y d.

Para encriptar se pasa el mensaje a binario y se lo divide en bloques de un cierto tamaño, cada bloque se encripta elevando el numero a la potencia e y reduciéndolo modulo n. Para desencriptar se eleva el código a la potencia d y se lo reduce modulo n.

El tamaño de los bloques es i tal que $10^{(i--1)} < n < 10^{i}$

Ejemplo (chiquito para poder seguir las cuentas) :

Sea p=5 , q=11, n=p*q=55,§(n)=40.

Elegimos d=23 pues 23 y 40 son relativamente primos.

Luego e=7 pues 7*23=161 (161 mod 40) = 1.

Si encriptamos números comprendidos en el rango (0..15) (tenemos 4 bits)

Número		Encriptado
0	0	(0^ 7 mod 55)
1	1	(1^ 7 mod 55)
2	18	(2^ 7 mod 55)
3	42	(3^ 7 mod 55)
4	49	(4^ 7 mod 55)
5	25	(5^ 7 mod 55)
6	41	(6^ 7 mod 55)
7	28	(7^ 7 mod 55)
8	2	(8^ 7 mod 55)
9	4	(9^ 7 mod 55)
10	10	(10^ 7 mod 55)
11	11	(11^ 7 mod 55)
12	23	(12^ 7 mod 55)
13	7	(13^ 7 mod 55)
14	9	(14^ 7 mod 55)
15	5	(15^ 7 mod 55)

Probar que el desencriptado funciona correctamente, por ejemplo para desencriptar el 42 debemos hacer 42^23, esta operación puede hacerse fácilmente sin usar números 'super enormes' ya que por cada producto aplicamos un modulo n.

42^2=4 42^4=16 42^8=36 42^16=31 42^17=37 42^18=14 42^19=38

42^20=1 42^21=42 42^22=4 42^23=3

Luego 3 mod 55 = 3 y queda desencriptado.

Notar que para calcular las potencias trabajamos siempre con aritmética modulo n.

El ejemplo presentado tiene algunas falencias que pueden ser descubiertas fácilmente por el lector (lo dejamos como ejercicio), estas fallas se reducen automáticamente a valores casi nulos cuando los números p y q son lo suficientemente grandes.

Criptoanálisis:

Las técnicas criptoanalíticas más utilizadas contra el RSA, aunque sin éxito, consisten en intentar factorizar el numero "n" que se distribuye en la clave publica averiguando de esta forma los números p y q. Debido a que no existen algoritmos eficientes para factorizar un número, el problema de descomponer un numero muy grande insume un tiempo tan elevado que los ataques mas sofisticados contra el RSA han fallado (o casi...)

El algoritmo RSA sin embargo presenta una vulnerabilidad: hay una leyenda que indicaría que el algoritmo es vulnerable. Y la clave de todo se la ha llevado a la tumba (una vez más) el misterioso Fermat.

4.4.2 PGP : Pretty Good Privacy.

En esta sección analizamos el programa más utilizado para encriptar y desencriptar datos mediante algoritmos de clave publica. El PGP se utiliza en internet y en casi todas las redes de mensajería cada vez que quiere transmitirse información privada.

PGP es un producto de distribución libre, es distribuido con sus fuentes y su distribución le ha causado a su autor Philip Zimmerman más de un problema como veremos más adelante.

PGP trabaja con el algoritmo RSA utilizando claves de 256,512 o 1024 bytes según el nivel de seguridad que se necesite, las claves de 1024 bytes superan ampliamente los mas estrictos requisitos militares sobre seguridad criptográfica.

PGP genera las claves públicas y privadas del usuario utilizando un algoritmo muy avanzado de pseudoaleatorización que mide los tiempos transcurridos entre lo que se tipea en un teclado. (PGP solicita al usuario que tipee durante un cierto tiempo en la pantalla) o los movimientos del mouse (se solicita al usuario que lo mueva aleatoriamente durante cierto tiempo).

La clave publica queda grabada en el disco y lista para ser distribuida, la clave privada se almacena también en el disco, PGP en sus manuales destaca que el acceso a la computadora donde se almacena la clave privada debe restringirse en forma drástica pues el conseguir la clave privada anula todo el sistema, el autor recomienda el uso de dispositivos que distorsionen las señales de radio en el ambiente donde reside la computadora pues existen dispositivos ultra-avanzados de las agencias gubernamentales que permiten leer la información de un disco a distancia mediante ondas de radio (!!).

Las claves publicas que nos envían otros usuarios son almacenadas en un conjunto de claves publicas (Public-key-ring) sobre el cual se pueden realizar altas, bajas y modificaciones.

Cuando un usuario le envía a otro su clave pública, por ejemplo a través de internet, el usuario que recibe la clave suele querer chequear que la clave publica recibida sea la del usuario que el quiere y no cualquier otra. Para ello PGP permite extraer de cada clave publica un numero conocido como 'FINGERPRINT' el Fingerprint puede ser chequeado telefónicamente o personalmente, y si coincide puede certificarse que la clave publica es de quien dice ser. (Cualquier cambio en la clave publica modifica el Fingerprint). El fingerprint se calcula hasheando la clave publica.

PGP dispone de varias opciones interesantes:

Envío de mensajes en forma clásica:

Este esquema sigue el mecanismo clásico de la encriptación por clave publica, el mensaje es encriptado usando la clave publica de un determinado usuario de forma tal que solo pueda ser desencriptado por la clave privada del mismo.

Certificación de mensajes:

Esta es una utilidad muy recomendable, y sirve para que un usuario firme un mensaje de forma tal que se pueda autenticar su autoría. Lo que hace el PGP es primero extraer un 'concentrado' del mensaje sometiéndolo a una función de hashing, luego el concentrado es encriptado con la clave privada del usuario y agregado al final del mensaje. Cuando el mensaje es recibido por un usuario la firma digital es desencriptada usando la clave pública del usuario y luego el mensaje es sometido a la función de hashing, si el concentrado coincide con el concentrado desencriptado del mensaje entonces el mensaje fue escrito por quien dice ser, de lo contrario o bien fue escrito por otra persona o bien fue modificado el texto del mensaje.

Los mensajes certificados a su vez pueden ser encriptados para que solo puedan ser leídos por una cierta persona.

Notar que la certificación utiliza el juego de claves en forma inversa al uso normal de las mismas.

Mensajes solo para sus ojos:

Esta opción del PGP permite encriptar un mensaje para una cierta persona de forma tal que cuando esta lo desencripte usando su clave privada el texto del mensaje solo se pueda ver en pantalla y no pueda ser grabado en un archivo, esta opción otorga una seguridad extra a quien envía el mensaje y tiene miedo que el usuario que lo recibe lo trate en forma descuidada dejándolo por allí.

Borrado especial del archivo a encriptar:

Cuando se quiere encriptar un mensaje muy critico que esta escrito en un archivo, PGP dispone de la opción de eliminar el archivo original del disco una vez encriptado. PGP no utiliza un borrado común del archivo sino que sobreescribe el área del disco con sucesivas pasadas de unos, ceros y unos y ceros alternados en forma random, esto lo hace varias veces. El algoritmo de borrado del PGP asegura que la información no podrá ser recuperada del disco. (Si el algoritmo no es lo suficientemente seguro el análisis de trazas magnéticas del disco puede permitir recuperar la información).

PGP es un programa sumamente seguro y es utilizado en todo el mundo para el envío de e-mail en forma segura y la certificación de mensajes de importancia.

4.4.3 El algoritmo RSA

Introducido por Ron Rivest, Adi Shamir y Len Adleman del MIT en 1978 el Algoritmo Rivest-Shamir-Adleman (RSA) es el único de los algoritmos de clave pública masivamente utilizados en la actualidad.

Los mensajes son encriptados en bloques que poseen un valor en binario menor o igual que un número n. Es decir en bloques de longitud menor o igual a $\log_2(n)$. La encriptación y desencriptacion se realiza de la siguiente manera, para un bloque de mensaje M y un mensaje cifrado C:

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Tanto el emisor como el receptor conocen el valor de *n*. el emisor conoce el valor de *e*, y el emisor el valor de *d*. por lo tanto este es un algoritmo con una clave pública {*e*,*n*} y una clave privada {*d*,*n*}

Generación de las claves

- Se seleccionan dos números primos, *p* y *q*

- Se calcula $n = p \times q$.
- Se calcula $\Phi(n) = (p-1)(q-1)$
- Se selecciona un entero usando: mcd $(\Phi(n),e) = 1$ y $1 < e < \Phi(n)$
- Se calcula $d = e^{-1} \bmod \Phi(n)$
- Clave Pública KU = $\{e,n\}$
- Clave Privada KR = $\{d,n\}$

Modelo criptografico cuantico

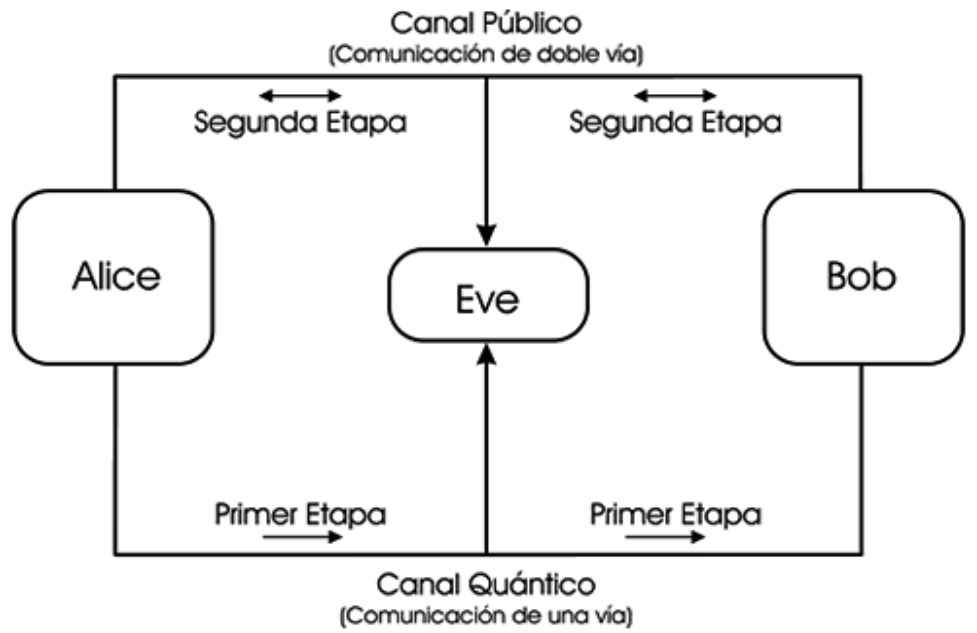
4.5 Principio y algoritmos

En general observar un sistema cuántico perturba al mismo, e impide que el observador conozca su estado exacto antes de la observación. Por lo tanto, si un sistema cuántico es utilizado para transferir información, alguien que quiera espiar la comunicación, o incluso el receptor previsto, podría verse impedido de obtener toda la información enviada por el emisor. Este rasgo negativo de la mecánica cuántica, conocido como principio de incertidumbre de Heisenberg, recientemente ha encontrado un uso positivo en el área de las comunicaciones privadas y seguras.

4.5.1 Principio básico de la criptografía cuántica

Como señalamos anteriormente, la criptografía cuántica se basa sobre el principio de incertidumbre de de Heisenberg. Veamos ahora como se puede aprovechar dicho principio para transmitir una clave en forma segura.

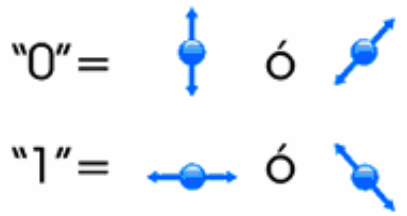
Figura 24 Diferencia de canales



La criptografía cuántica hace uso de dos canales de comunicación entre los dos participantes. Un canal cuántico, el cual tiene un único sentido y que generalmente es una fibra óptica. El otro es un canal convencional, público y de dos vías, por ejemplo un sistema de comunicación por radio que puede ser escuchado por cualquiera que desee hacerlo.

Supongamos que Alice desea enviar una clave a Bob a través de un canal cuántico. El valor de cada bit es codificado dentro de una propiedad de un fotón, por ejemplo su polarización. La polarización de un fotón es la dirección de oscilación de su campo eléctrico. Esta polarización puede ser, por ejemplo, vertical, horizontal o diagonal (+45º y -45º).

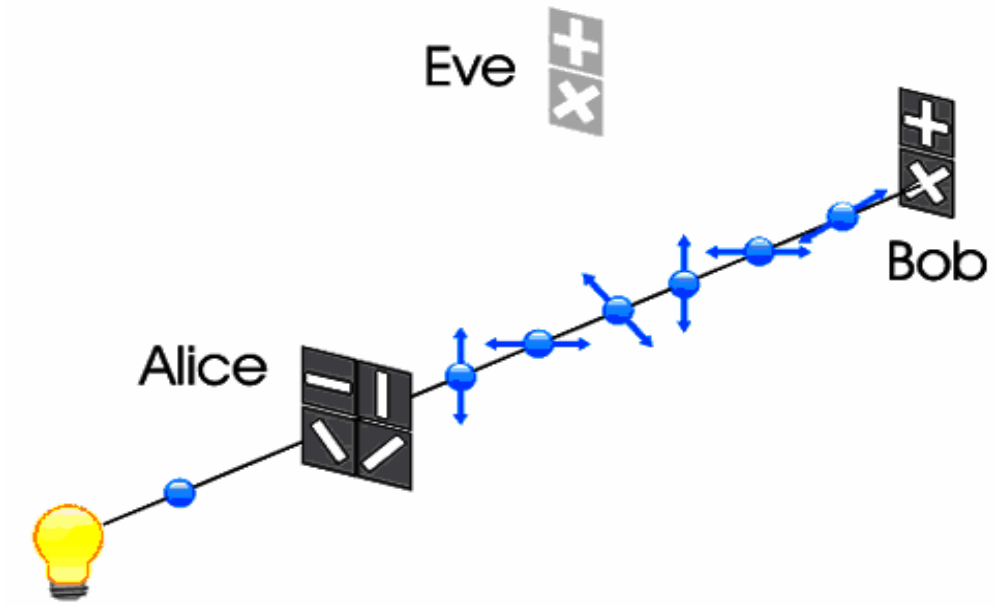
Por ejemplo, Alice y Bob se ponen de acuerdo en que:



Un filtro puede ser utilizado para distinguir entre fotones verticales u horizontales. Otro filtro se utiliza para distinguir entre fotones diagonales (+45º y -45º).

Cuando un fotón pasa por el filtro correcto, su polarización no cambia. En cambio cuando un fotón pasa a través de un filtro incorrecto, su polarización es modificada en forma aleatoria.

Figure 25 Filtros de Fotones



Por cada bit de la clave, Alice envía un fotón, cuya polarización es elegida de forma aleatoria. Las orientaciones seleccionadas son almacenadas por Alice.

Por cada fotón recibido, Bob elige de forma aleatoria cual filtro se va a utilizar y se registran el filtro seleccionado y el valor de la medición.

Una vez que se han intercambiado todos los fotones, Bob le revela a Alice a través de un canal convencional la secuencia de filtros que utilizo durante la transmisión de fotones. Luego Alice le dice a Bob en qué casos eligió el filtro correcto. En éste momento ambos saben en que casos sus bits

deberían ser idénticos, es decir cuando Bob utilizo el filtro correcto. Estos bits formarán la clave final.

Si Eve intenta espiar la secuencia de fotones, al no conocer de antemano si la polarización del próximo fotón es diagonal o rectilínea, no podrá medirlo sin correr el riesgo de perturbarlo de tal forma que se introduzca un error.

Finalmente, Alice y Bob verifican el nivel de error de la clave final para validarla. Esto lo hacen haciendo públicos una cierta cantidad de bits. Si encuentran diferencias en sus bits, tienen una razón para sospechar que están siendo espiados y deberán descartar todos los datos y comenzar nuevamente el intercambio de fotones. Si coinciden y si se compararon una cantidad lo suficientemente grande de bits, pueden estar razonablemente seguros de que las partes que no han sido comparadas abiertamente en el canal inseguro son de hecho un secreto compartido y pueden conformar una clave secreta para ser utilizada en la transmisión de mensajes con significado. La transmisión de mensajes con significado se realiza sobre el canal publico o inseguro utilizando cualquier método de clave privada que crean conveniente por ejemplo DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).

Por el momento no existe un sistema con el cual se puedan mantener comunicaciones por un canal cuántico. Por lo tanto la aplicación de la criptografía cuántica se ve restringida a la distribución de claves. Sin embargo, la transmisión olvidadiza puede ser utilizada como base para construir algoritmos de Zero Knowledge proofs y bit commitment.

4.5.2 El Algoritmo BB84

El esquema de codificación BB84 fue el primer codificador cuántico de información clásica en ser propuesto de forma tal que el receptor, legitimo o ilegitimo, pueda recuperar con 100% de confiabilidad. Esta es la base sobre

la cual están fundados la mayoría de los protocolos cuánticos. El ejemplo que se vio anteriormente en la introducción a la criptografía cuántica se basa en este algoritmo.

1. La fuente de luz, generalmente un LED (Light emitting diode) o láser, es filtrada para producir un rayo polarizado en ráfagas cortas y con muy baja intensidad. La polarización en cada ráfaga es entonces modulado por el emisor (Alice) de forma aleatoria en uno de los cuatro estados (horizontal, vertical, circular-izquierdo o circular-derecho).
2. El receptor, Bob, mide las polarizaciones de los fotones en una secuencia de bases aleatoria (rectilíneo o circular).
3. Bob le dice públicamente al emisor que secuencia de bases utilizo.
4. Alice le dice al receptor públicamente cuales bases fueron elegidas correctamente.
5. Alice y Bob descartan todas las observaciones en las que no se eligió la base correcta.
6. Las observaciones son interpretadas usando un esquema binario por ejemplo: horizontal o circular-izquierdo es 0, vertical o circular-derecho es 1.

Este protocolo se complica con la presencia de ruido, el que puede ocurrir en forma aleatoria o ser introducido por una escucha. Con la existencia de ruido las polarizaciones observadas por el receptor pueden no coincidir con las emitidas por el emisor. Para lidiar con esta posibilidad, Alice y Bob deben asegurarse que poseen la misma cadena de bits. Esto se realiza usando una busqueda binaria con verificación de paridad para aislar las diferencias. Con el descarte del último bit de cada comparación, la discusión pública de la paridad se vuelve inofensiva. En el protocolo de Bennett de 1991 este proceso es:

1. Alice y Bob acuerdan una permutación aleatoria de las posiciones de los bits en sus cadenas, para distribuir aleatoriamente la posición de los errores.

2. Las cadenas se parten en bloques de longitud *k*, con *k* elegido de forma tal que la probabilidad de múltiples errores por bloque sea muy baja.
3. Por cada bloque, Alice y Bob computan y anuncian públicamente las paridades. Luego el último bit de cada bloque es descartado.
4. Para cada bloque en el que difirieron las paridades calculadas, Alice y Bob usan una búsqueda binaria con log(*k*) iteraciones para localizar y corregir el error en el bloque.
5. Para contemplar múltiples errores que aún no han sido detectados, los pasos 1 al 4 son repetidos con tamaños de bloque cada vez más grandes.
6. Para determinar si aun quedan errores, Alice y Bob repiten un chequeo aleatorio:

    - Alice y Bob acuerdan públicamente una muestra de la mitad de las posiciones en sus cadenas de bits.
    - Públicamente comparan las paridades y descartan un bit. Si las cadenas difieren, las paridades van a discrepar con probabilidad ½.
    - Si hay discrepancias, Alice y Bob utilizan una búsqueda binaria para encontrarlas y eliminarlas.

7. Si no hay desacuerdos después de *l* iteraciones, se concluye que sus cadenas coinciden con una probabilidad de error de 2^{-l}.

Ejemplos del algoritmo BB84

Notación utilizada

Tipos de Medición	Resultados de medición de fotón
 Rectilínea	 Circular-izquierda
Circular	 Circular-derecha
	 Vertical
	 Horizontal

4.5.3 Transmisión sin escuchas

Alice enviara una secuencia de 24 fotones. La probabilidad de que el detector de Bob Falle es del 40% Alice envía la siguiente secuencia de fotones:

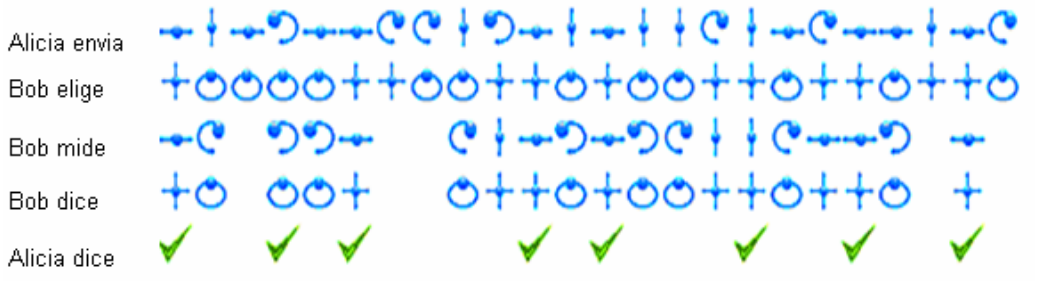
Bob decide aleatoriamente si va a realizar una medición rectilínea o circular para cada fotón que Alice envié. La secuencia elegida es:

Por cada medición, existe una probabilidad del 0.4 (40%) de que el detector ni siquiera detecte el fotón. Los resultados de las mediciones son:

Luego, Bob le dice a Alice a través del canal público que tipo de mediciones (rectilínea o circular) ha logrado hacer exitosamente, pero no el valor de las mediciones.

Alice le dice a Bob, también por el canal público, cuales de las mediciones fueron del tipo correcto.

Como Bob solo va a hacer el mismo tipo de medición que Alice la mitad de las veces, y dado que la probabilidad de que el detector falle en leer un fotón es del 40%, se espera que unos 7.2 de los 24 dígitos compartidos sean utilizables. De hecho en éste ejemplo se generaron 8 dígitos utilizables. En resumen:



4.5.4 Transmisión con escuchas

Alice enviara una secuencia de 24 fotones. La probabilidad de que el detector de Bob Falle es del 40%. Alice envía la siguiente secuencia de fotones:

Eve decide aleatoriamente si va a realizar una medición rectilínea o circular para cada fotón que Alice envié. La secuencia elegida es:

Por cada medición, existe una probabilidad del 0.4 (40%) de que el detector ni siquiera detecte el fotón. Los resultados de las mediciones de Eve son:

Bob decide aleatoriamente si va a realizar una medición rectilínea o circular para cada fotón que Alice envié. La secuencia elegida es:

Por cada medición, existe una probabilidad del 0.4 (40%) de que el detector ni siquiera detecte el fotón. Los resultados de las mediciones de Bob son:

Luego, Bob le dice a Alice a través del canal público que tipo de mediciones (rectilínea o circular) ha logrado hacer exitosamente, pero no el valor de las mediciones.

Alice le dice a Bob, también por el canal público, cuales de las mediciones fueron del tipo correcto.

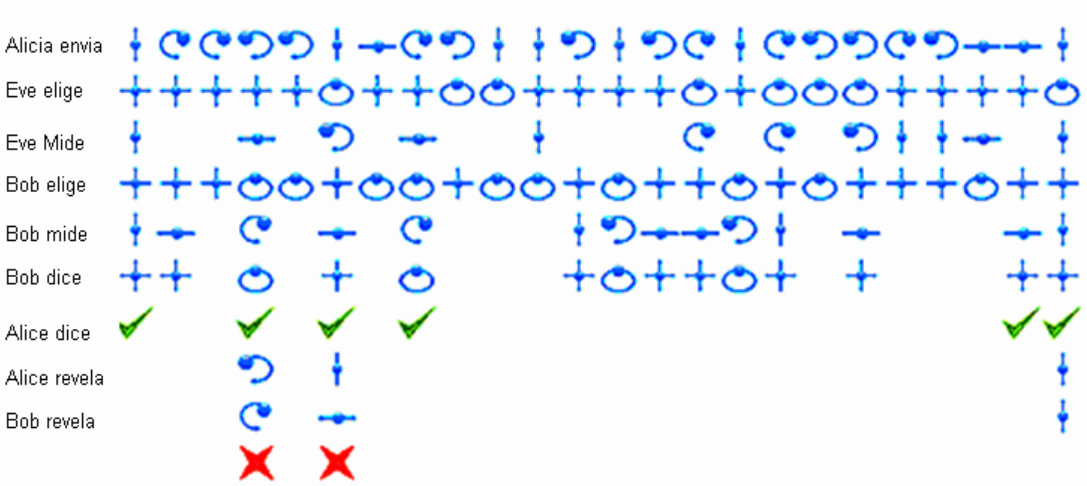
Como Bob solo va a hacer el mismo tipo de medición que Alice la mitad de las veces, y dado que la probabilidad de que el detector falle en leer un fotón es del 40%, se espera que unos 7.2 de los 24 dígitos compartidos sean utilizables. De hecho en éste ejemplo se generaron 6 dígitos utilizables.

Bob y Alice quieren saber si alguien ha estado escuchando su comunicación, para lo cual comparten el 50% de los dígitos compartidos. Se va a seleccionar una muestra al azar para que ningún espía pueda predecir que dígitos van a ser verificados y evite modificarlos.Alice revela primero el 50% de sus dígitos:

Bob le indica a Alice cual es el valor que midió para los mismos dígitos

Como 2 de los 3 dígitos verificados son incorrectos, Alice y Bob saben que alguien estuvo escuchando su intercambio de fotones.

En resumen:



4.5.5 Criptografía cuántica olvidadiza y transferencia comprometida

En un modelo de transmisión olvidadiza 1 de 2 (oblivious transfer, OT), una de las partes, Alice, tiene 2 bits b_0, b_1 los cuales envía a la otra

parte, Bob, pero Bob solo puede obtener 1 de los 2 bits. Sin embargo, Alice no puede saber cual de los 2 bits es el que recibió Bob.

De forma análoga en un modelo de transmisión olvidadiza m de n, Alice envía n bits a Bob pero Bob solo puede obtener m de los n bits. Sin embargo, Alice no puede saber cuales son los m bits que recibió Bob.

Este tipo de transmisión puede ser utilizado como base para la construcción de otros protocolos criptográficos. Un ejemplo es la contracción de pruebas de cero-conocimiento (zero-knowledge proofs). Que son una forma de probar algo, por ejemplo que uno posee un permiso válido, sin revelar información adicional al receptor.

En una transferencia olvidadiza comprometida, (Committed Oblivious Transfer, cot), supongamos que Alice está comprometida a los bits a_0 y a_1 y Bob esta comprometido a b luego de ejecutar cot $(a_0 . a_1)(b)$, Bob va a estar comprometido a que $a = a_b$. Sin importar lo que haga, Alice no va a poder utilizar el protocolo para aprender información de b, y Bob sin importar que haga no va a poder utilizar el protocolo para aprender información de a_b.

Este tipo de transmisión permite que cada una de las partes involucradas en una transferencia olvidadiza esté segura que la otra parte esta realizando la operación de transferencia olvidadiza en las entradas declaradas.

CONCLUSIONES

1. A pesar de que en estos momentos la computación cuántica está en laboratorios y la mayoría con cambios de conceptos y pruebas esta será lo que logrará que pasemos de computadores de chips a la computadora cuántica

2. Los sistemas cuánticos son en estos momentos a lo que nos hace soñar, si los aplicamos al campo de la computación que de igual forma nos deja soñar, si los hacemos realidad se podrán alcanzar casi cualquier sueño

3. La criptografía es la rama en la cual la computación cuántica ha sobresalido, por ser el área de mayo fácil acoplamiento de este gran nuevo concepto.

RECOMENDACIONES

1. En realidad la aplicación de la criptografía cuántica es inmenso en el mundo actual se puede hablar de comunicación de radio, celular y satelital, transmisión de información inter-empresas, no solo bancos, sino aseguradoras, empresas internacionales, compras por Internet.

2. Con métodos como el encriptamiento cuántico la gente se volcará a hacer mas transacciones por esto método de Negocios, el E-BUSSINES mas seguro que puede existir.

3. El campo de las comunicaciones es el mas creciente, en este momento, el aparecimiento de los celulares ha hecho que la gente cambie su habito de comunicación y, con ello, muchos mas hábitos mas. Primero el Celular, el roaming internacional para estar mas comunicados solo con un numero, con ello, también, la creación de los celulares satelitales para no perder señal en cualquier isla y cualquier parte del mundo, la aparición del internet por celulares (WAP, GPRS) el mail y las transacciones en línea -GPS seguro- el estar en Internet móvil y poder por medio de una computadora o de un celular o una agenda –Blackberry- en línea con las personas, así como las herramientas OTA -on the Air- para enviar información entre los teléfonos de GSM y con los negocios hace necesario el poder encriptar la comunicación de estos dispositivos. Es allí donde entra el método de encriptamiento cuántico, debido que con el crecimiento y el auge que toma la comunicación y ofreciéndoles a los clientes la seguridad de que su información viajara por un canal seguro que nadie podrá descifrar.

BIBLIOGRAFÍA

Libros

Mika Hirvensalo, Quantum Computing (Natural Computer Series), Springer, 2001

Julian Brown, The Quest for the quantum computer, Simon &Schuster, 2001

Michael Brooks, Quantum Computing and Comunications, Springer-Verlag, 1999

Robert Wright, Three Scientists and Their God: Loking from Meaning ina an Age of Information, Times Bookx, 1998

Referencias electrónicas

Mecánica Quántica

http://caminantes.metropoliglobal.com/web/cuant/curscuant.html#intro

http://www.astrocosmo.cl/h-foton/h-foton-06_03.htm

http://es.wikipedia.org/wiki/Mec%E1nica_cu%E1ntica

Física Quántica

http://www.geocities.com/fisica_que

Computación Cuantica

http://www.qubit.org/

http://perso.wanadoo.es/nancarrow/contents/q_comp/

http://quantum.fis.ucm.es/

http://www-users.cs.york.ac.uk/~schmuel/comp/comp.html

http://delta.cs.cinvestav.mx/~gmorales/quantum/intro.html

Criptografia

http://www.portalmundos.com/mundoinformatica/seguridad/cuantica.htm

http://www.vivalinux.com.ar/articulos/1089.html

ANEXOS

Puertas Lógicas

Una puerta lógica binaria es un sistema de dos entradas (x,y) que regresa un valor f(x,y) función de ellas. Hay dos bits de entrada por cada una de ellas, lo cual nos lleva a cuatro combinaciones posibles en la entrada. A cada una de esas cuatro combinaciones pueden responder con un cero o uno, esto nos lleva a 16 posibles funciones.

Medida de la información.

El primer problema que nos deberíamos plantear es el de la medida de la información. Parece intuitivo decidir en qué medida se conoce un sistema, pero se necesita una formalización. La pregunta puede plantearse en unos términos sencillos

Supóngase que dan el valor de un cierto número, X. ¿Cuánta información obtenemos a partir de esto?
Bien, esto depende de lo que se supiese previamente acerca ese número. Por ejemplo, ya se sabía el valor. En tal situación se habría aprendido, exactamente, nada. Por otra parte, pongamos que sabíamos que el valor X es obtenido al tirar un dado. En este otro caso desde luego que habremos obtenido información.

Una observación: una medida de la información es, a su vez, una medida de la ignorancia, puesto que la información que, dependiendo del

contexto, contenga X, es precisamente la que ganaríamos al conocer su valor, y por lo tanto parte de la incertidumbre inicial.