Inter*net* Electronic Journal*

Nanociencia et Moletrónica

Diciembre 2009, Vol. 7, N°2, pp. 1379-1388

# Internet Cuántico

**H. E. Caicedo-Ortiz**

Universidad del Cauca, Popayan, **Colombia**
Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional, Sede Zacatenco
Ciudad de México, **México**
e-mail: hecaicedo@esfm.ipn.mx

recibido: 03.10.09 revisado: 15.10.09 publicado: 31.12.09

Citation of the article;
H. E. Caicedo-Ortiz, Internet Cuántico Internet Electron. J. Nanoc. Moletrón. 2009, Vol. 7, N° 1, pp 1379-1388

# Internet Cuántico

**H. E. Caicedo-Ortiz**

Universidad del Cauca, Popayan, **Colombia**
Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional, Sede Zacatenco
Ciudad de México, **México**
e-mail: hecaicedo@esfm.ipn.mx

recibido: 03.10.09 revisado: 15.10.09 publicado: 31.12.09

*Internet Electron. J. Nanoc. Moletrón., 2009, Vol. 7, N°2 , pp. 1379-1388*

**Resumen**

En este artículo se describe cómo es posible extender la idea de red computacional hacia la computación e información cuántica. De forma adicional, se busca motivar a que investigadores en el campo de redes y protocolos de información a emplear su experiencia en el desarrollo de nuevas tecnologías de información cuántica.

***Palabras clave:*** *Internet Cuántico, Redes Cuánticas, Computación Cuántica, Información Cuántica, Criptografía Cuántica, Protocolos de Última Generación.*

**Abstract**

This paper describes how to extend the idea of a computing network to quantum information and computing. Also it seeks to motivate researchers in the field of nets and protocols to use their experience in the development of new quantum information technologies.

***Keywords:*** *Quantum Internet, Quantum Network, Quantum Computing, Quantum Information.*

Internet Electron. J. Nanoc. Moletrón. 2009, Vol. 7, N° 1, pp 1379-1388

## 1. Introducción

La Computación Cuántica y la Teoría de la Información Cuántica [1] son una excitante área de investigación y un desafío intelectual que toca los fundamentos de la ingeniería, la informática y la física cuántica, ofreciendo velocidades de procesamiento y capacidad de almacenamiento de información mucho mayores que las logradas e imaginadas hasta la fecha, convirtiéndose en una de las líneas con mayor desarrollo técnico, científico y tecnológico. El modelo de computabilidad ofrecido por estas teorías proporciona el primer desafío creíble de la Tesis modificada de Church-Turing[1], la cual establece que cualquier modelo razonable de computación puede ser simulado eficazmente por una Máquina de Turíng probabilística [2].

La potencialidad de este nuevo esquema en comparación con la computación clásica, radica en que su escenario de trabajo no solo se restringe a dos únicos estados de operación (0,1), al contrario, se puede obtener multitud de estados intermedios como resultado de la superposición de estas dos posibilidades. Esto trae consigo que al ser realizada una operación, el sistema permita evaluar todas las posibilidades en un solo paso, es decir, realizar una computación en paralelo, lo que se traduce en reducción del tiempo y aumento en la velocidad de procesamiento.

Con la aparición de los protocolos de comunicación cuántica en 2001 [3] que son más poderosos que los alcanzados clásicamente y con la primera implementación experimental de un memoria cuántica por luz en 2004 [4], aparece la idea de poder interconectar componentes de procesamiento cuántico de una forma eficiente, los cuales operarían como una gran red cuántica.

En este artículo se describe una selección de algunos componentes que constituyen a un ordenador cuántico, al igual que los equipos y protocolos necesarios para construir una gran red cuántica, tomando como referencia los dispositivos utilizados en la actualidad por las redes convencionales.

## 2. Computación Cuántica

### 2.1. El qubit

Al igual que en los sistemas clásicos de computo en los cuales la mínima unidad de información es el bit, en la teoría de la computación cuántica este elemento tiene su contraparte y se denomina bit cuántico ó qubit [1]. Aunque esta entidad se describe como un objeto matemático con ciertas propiedades específicas, tiene una realidad física y tangible, la cual se la cual se representa a través de un sistema cuántico de dos estados, pero en el cual todo su tratamiento es enteramente abstracto, dando libertad de generar una teoría general de la computación e información que no depende del sistema físico que se emplee para su implementación. Al considerar sistemas de esta clase como mínimas unidades de información, es necesario para su correcta descripción, implementar el formalismo matemático de la mecánica cuántica. Aunque

existen varios esquemas que describen los estados de un sistema cuántico, el más conveniente y conciso es la notación de Dirac [8], la cual se ha convertido en un estándar en la física moderna, donde cualquier estado es representado por un vector ket, denotado por $|\psi\rangle$y las operaciones sobre los estado se realizan a través de operadores que son transformaciones lineales que actúan sobre el ket.
Considerando esta representación, los dos estados posibles para un qubit son $|0\rangle$ y $|1\rangle$ ó matricialmente $\begin{pmatrix}1\\0\end{pmatrix}$y $\begin{pmatrix}0\\1\end{pmatrix}$, que corresponden en analogía al 0 y 1 de un bit clásico, donde tales vectores pertenecen a un espacio de Hilbert $L^2$ [1].
Como se mencionó, la potencialidad de este esquema radica en que el qubit puede tomar otro valor diferente a los dos antes mencionados, siendo esto posible a la combinación lineal de estados, por lo cual un qubit en su forma más general presenta la forma

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle, \quad (1)$$

donde $a_0$ y $a_1$ son números complejos que satisfacen la relación de normalización $|a_0|^2 + |a_1|^2 = 1$.
La habilidad de un sistema cuántico de existir simultáneamente en una mezcla de todos los estados permitidos es conocida como "Principio de Superposición" [1] y es una característica completamente cuántica. Esto significa que mientras en un sistema clásico el bit tiene una información concreta a la cual se puede acceder sin perturbarla, el qubit siempre proporciona un resultado probabilístico.

Consideremos ahora la situación en la cual hay más de un qubit, es decir, un registro cuántico. En tal situación, el espacio de estados es el resultado del producto tensorial de los espacios asociados a cada uno de los qubits. Si estos se representan por $L_1^2$ y $L_2^2$ de dimensiones *n* y *m* respectivamente, el nuevo espacio vectorial es $L_{12}^2 = L_{12}^2 \otimes L_{12}^2$ de dimensión *mn* que a su vez es el número de elementos de la base. Tomando el caso particular de un sistema de registro cuántico de 2 qubits (2-qubits) en el cual la dimensión del espacio es $2^2 = 4$, su base natural esta constituida por 4 vectores $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Aquí el qubit $|\psi\rangle$ se describe de acuerdo a la superposición coherente

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle, \quad (2)$$

Donde $a_{ij}$ es un número complejo. De esta manera, para representar completamente el estado del sistema es necesario 4 subestados, cada uno asociado a número complejos. Considerando ahora un sistema de N- qubits, la base consta de $2^N$ elementos de estados accesibles. En forma más general, tomando cada uno de los elementos de la base mediante el ket $|x\rangle$ con $x = 1, 2, 3, ..., 2^N - 1$, el qubit se puede representar así

$$|\psi\rangle = \sum_{x=0}^{2^N - 1} a_x |x\rangle \,, \tag{3}$$

Es vital considerar que no es correcto tratar de dar una interpretación al qubit desde un punto de vista probabilístico de la teoría clásica de la computación, debido a que esa aparente complejidad en la descripción de estos sistemas es la encargada de presentar las mayores ventajas con respecto al modelo clásico. Es así como en el estado cuántico que se describe por las ecuaciones (1) - (3), no solamente hay una combinación probabilística de cada estado, si no que adicionalmente se incorporan los efectos cuánticos como la interferencia y el entrelazamiento, los cuales permiten realizar un masivo procesamiento de información que se traduce en un aumento exponencial en la velocidad de calculo con respecto a los dispositivos clásicos en los cuales esta característica es de tipo polinomial.

## 2.2. Compuertas Cuánticas

De la misma forma que en la electrónica convencional, en computación cuántica existen circuitos que realizan y llevan a cabo los procesos de cómputo. En este esquema, una compuerta lógico cuántica es una función que realiza un operador unitario en un conjunto de qubits seleccionados en un cierto periodo de tiempo. En la teoría clásica las compuertas lógicas constituyen un conjunto claramente finito [9], debido a que el espacio de estados de un qubit es continuo, el número de posibles transformaciones unitarias también lo es, y, en consecuencia, existen infinitas compuertas cuánticas. Sin embargo, es posible demostrar [10] que cualquier transformación unitaria en un conjunto de N qubits puede realizarse mediante la aplicación sucesiva de tan sólo dos compuertas cuánticas: la asociada a la operación ***XOR***, y la de rotación, $\hat{\mathrm{R}}=(\theta,\phi)$.

El operador ***XOR*** es un caso particular de un conjunto de operadores que actúan sobre un par de qubits y que pueden ser representados mediante la expresión

$$|\psi\rangle = a_{00}|0\rangle\langle 0|\hat{I} + |1\rangle\langle 1|\hat{U} \,, \tag{4}$$

donde $\hat{U}$ representa una transformación unitaria cualquiera sobre un único qubit. Es decir, mientras que el primer qubit permanece inalterado, al segundo se le aplica $\hat{I}$ ó $\hat{U}$ dependiendo del estado del primero.

Una característica muy importante que presentan los circuitos cuánticos es su capacidad de hacer computación reversible. Para entender este concepto, es necesario considerar un esquema donde el procesamiento de información se realiza al interior de una caja negra con igual conjunto de líneas de entrada y salida, es decir, por cada línea de entrada hay una y solo una línea de salida, la cual esta predeterminada por su entrada. En la situación más trivial, las señales simplemente se propagan a través de la caja sin modificarse. En estas circunstancias, la salida no lleva más información que la entrada. Si se conoce la salida, es posible calcular la entrada, por lo cual se dice que la computación de este proceso es reversible. Muy distinto es lo que ocurre con una

compuerta lógica convencional, como por ejemplo la compuerta AND. Para este caso se tienen dos líneas de entrada y solo una de salida. Hay tres posibles estados que pueden conducir a una salida cero. Por lo tanto se ha perdido irremediablemente información sobre la entrada y consecuentemente la compuerta AND es irreversible. Esta reducción en el espacio de fase de las entradas hacia las salidas trae consigo una forzosa disminución de la entropía o grado de desorden del sistema, lo cual es compensado con la generación de calor, por consiguiente, sistemas no reversibles se calientan [11].

En 1982, Charles Bennett de IBM demostró que sistemas de computo reversible operan como maquinas de Carnot, donde los procesos de perdida de energía por disipación de calor son mínimos [12]. Desde el punto de vista nanoscópico, las compuertas cuánticas si son reversibles debido que al estar descritas las operaciones que ellas realizan por operadores unitarios, estos procesos de reversibilidad aparecen de forma natural, por consiguiente es de esperar que los sistemas de computo mecánico cuántico presenten además de una alta velocidad de procesamiento una mayor eficiencia termodinámica, con un mínimo de consumo de energía.

### 2.3. Memoria Cuántica

Hasta hace algunos años, los dispositivos de computo cuántico tan solo podían en teoría procesar información, más no almacenarla. En el año 2004, un grupo integrado por científicos del Niels Bohr Institute, en Dinamarca, y el Max-Planck-Institut für Quantenoptik, en Garching, Alemania, desarrollaron una técnica experimental a través de la cual es posible almacenar impulsos de luz en átomos mediante un protocolo que confiere a la información almacenada un 70% de confiabilidad [4].

Esta memoria atómica, equivalente a una memoria ram de cualquier computadora actual, fue creada con un sistema gaseoso de átomos de Cesio, logrando retener información por cuatro milisegundos, lo cual significa que el ruido cuántico presente en el sistema durante este tiempo es mínimo, permitiendo que dos propiedades de la luz como lo son su amplitud y fase pueden transferirse a la materia con gran fidelidad. Este hecho, aparentemente sencillo abre la posibilidad de crear una red constituida por computadores cuánticos, en la cual la transmisión de información se realiza a través de fotones por canales clásicos como lo es la fibra óptica, pero para ello es necesario contar con otro elemento de vital importancia y es la Repetidora Cuántica, la cual será descrita y analizada en la siguiente sección.

## 3. Repetidoras Cuánticas

Al pensar en una red de computadores convencional, un componente esencial de este tipo de sistemas lo constituye un elemento que amplifique y replique la señal en su trayecto de un emisor hacia un receptor a grandes distancias. Este dispositivo se denomina repetidora y en un esquema de una Internet Cuántica, su construcción presenta grandes desafíos, ello debido a que una señal cuantica arbitraria debe

preservar su naturaleza cuántica, lo que significa que no es posible emplear los métodos convencionales de amplificación para tal fin.

A pesar de todo lo mencionado, la construcción de estos dispositivos puede ser alcanzada, para ello se emplea una característica de los sistemas cuánticos conocida como entrelazamiento (entanglement), en la cual dos partículas subatómicas, permanecen indefectiblemente interrelacionadas, si han sido generadas en un mismo proceso. Estas partículas forman subsistemas que no pueden describirse separadamente. Cuando una de las dos partículas sufre un cambio de estado, la otra lo sufre automáticamente, lo cual sucede de forma instantánea y con independencia de la distancia que las separe en ese momento. Para que esta característica sea empleada en redes cuánticas a grandes distancias, es necesario emplear un entrelazamiento compartido, el cual permite realizar el teletransporte de un estado cuántico arbitrario [14]. El canal físico por donde se envía la información que permitirá interconectar los distintos computadores cuánticos es igual al empleado en las grandes redes como lo es la fibra óptica. Un esquema de repetidora cuántica puede ser llevado a cabo dividiendo el canal físico en pequeños segmentos, cuya longitud es determinada teniendo en cuenta las posibles perdidas de información debidas a efectos de decoherencia o de desorden de los qubits. Los segmentos son conectados por nodos que son procesadores cuánticos operando con unos cuantos qubits, los cuales almacenan los estados cuánticos y realizan operaciones cuánticas que preservan el entrelazamiento, de tal manera que la información puede ser transferida de segmento a segmento. La fidelidad de la información en este tipo de sistemas puede ser manejada por un protocolo de purificación de entrelazamiento, tal como fue propuesto por el grupo de Bennett en 1996 [14].

En la actualidad existen diversos esquemas tanto teóricos [15] como experimentales [16-17] para la creación de repetidoras cuánticas, sobresaliendo de entre ellos una reciente demostración de teleportación de alta fidelidad de fotones en una fibra óptica a través del río Danubio en Viena, Austria en 2004[18], lo que pronostica que en pocos años este tipo de dispositivos serán una realidad.

## 4. Red De Ordenadores Cuánticos

Se puede visualizar a futuro una internet cuántica que consiste de ordenadores cuánticos (nodos) conectados por canales de comunicación clásicos (fibra óptica). Cada uno de estos nodos tiene como función almacenar qubits con información cuántica y procesarla localmente empleando para ello compuertas cuánticas. La información es intercambiada entre los nodos a través, nuevamente, de canales clásicos. Los métodos de almacenamiento y procesamiento de información son implementados físicamente en qubits materiales como lo son las trampas de iones o átomos [19], junturas superconductoras Josephson [20] y espín nuclear o electrónico en puntos cuánticos [6], siendo estos últimos los de mayor interés en el campo tecnológico, debido a que se basan en materiales semiconductores, lo cual permite pensar en crear a futuro tecnologías hibridas. La transferencia de información cuántica sobre una cierta distancia

es mejor realizarla por medio de qubits volátiles, por ejemplo estado de polarización de fotones. Un componente clave de tal red es una interfaz cuántica entre qubits estacionarios y volátiles, por ejemplo la conversión del estado cuántico del qubit estacionario en un qubit volátil y lo inverso, con una alta fidelidad.

La primera propuesta teórica para realizar transferencia de estados cuánticos entre qubits volátiles y estacionarios y distribución de entrelazamiento entre los nodos distantes fue dada por el grupo de Cirac en 1997 [21] y cuya aproximación experimental esta siendo implementada en el Caltech MURI Center for Quantum Networks [22], así como en la Universidad de Michigan.

A pesar que el desarrollo de un procesador cuántico capaz de llevar a cabo tareas y operaciones no posibles por los dispositivos convencionales esta muy lejos de ser alcanzado en los próximos 30 años, procesadores cuánticos de pocos qubits como los construidos en los últimos 6 años podrían ser el primer paso para alcanzar este objetivo. Así, una red cuántica constituida por este tipo de procesadores daría lugar a una computación cuántica distribuida, consistente en un dispositivo multiprocesador y en el cual cada uno de los pequeños procesadores tan solo operaria con unos pocos qubits pero en conjunto todo el sistema interconectado a través de una red cuántica operaria como un gran dispositivos de cómputo mecánico cuántico efectivo.

Un análogo clásico de este tipo de arquitectura es la empleado por el proyecto SETI (*Search for ExtraTerrestrial Intelligence*, o Búsqueda de Inteligencia Extraterrestre), liderado por la Universidad de Berkeley [23] y en el cual se emplea la técnica de computación distribuida, de manera que se conjuga la potencia de muchas máquinas a lo largo de todo el planeta que utilizan un software como descansa pantalla para analizar señales captadas por el radio telescopio de Arecibo, Puerto Rico y buscar patrones que no obedezcan a la aleatoriedad. En la actualidad, hay alrededor de 4 millones de usuarios con el programa SETI instalado en sus computadores, todas ellas interconectadas a través de internet y conformando una gran supercomputadora procesadoras de señales de radio espaciales.

## 5. Conclusiones

La realización de un dispositivo de computo mecánico cuántico, robusto y escalable, es decir, con los suficientes qubits necesarios para llevar a cabo tareas similares a las hechos por los dispositivos de computo convencionales solo se vislumbra a unos 30 años. Con la implementación de redes cuánticas, constituidas por pequeños procesadores cuánticos que operan con unos pocos qubits y haciendo el papel de nodos, la idea de implementar un gran ordenador cuántico se convierte en una realidad menos lejana. En este punto, es necesario que expertos científicos e ingenieros de los campos de protocolos y las redes se sumen a esta nueva aventura, en la cual las ganancias en el campo científico y tecnológico claramente superan y con creces la actual tecnología, abriendo nuevos paradigmas en el procesamiento de la información.

**REFERENCIAS**

[1] M. A. Nielsen and I. Chuang, "Quantum Computation and Quantum Information, *Cambridge University Press*, (1st edition). United Kingdom: 2001.
[2] D. Deutsch, "Quantum theory, the Church-Turing Principle and the universal quantum computer" Proc. R. Soc. London A, vol 400, p 97, 1985.
[3] L.-M. Duan , M. D. Lukin, J. I. Cirac and P. Zoller, " Long distance quantum communication with atomic ensembles and linear optics". *Nature*, vol 414, p 413, 2001.
[4] B. Julsgaard, J. Sherson, J.I. Cirac, J. Fiurasek and E. S. Polzik, "Experimental demonstration of quantum memory for light," *Nature,* vol 432, p 482, 2004.
[5] D. Cory, A. F. Fahmy and T.F. Havel, "Ensemble quantum computing by NMR spectroscopy", *Proc. Natl. Acad. Sci. USA,* vol 94, :p 1634, 1997.
[6] D. Loss and P. DiVincenzo,"Quantum computation with quantum dots", *Phys. Rev. A.*, vol 57, pp120-126, 1998
[7] H.E.Caicedo-Ortiz and S.T.Perez-Merchancano, "Exchange Energy in Coupled Quantum Dots", Brazilian Journal of Physics., vol 36, No 3B pp 874-877, 2006.
[8] P. Dirac, "Principios de Mecánica Cuántica". *Editorial Arial*, 1967.
[9] P. Benioff, "Quantum mechanical hamiltonian models of turing machines", *J. Stat. Phys*, vol 29, p 515, 1982.
[10] D. DiVincenzo, "Two-bit gates are universal for quantum computation", *Phys. Rev. A.*, vol 51, p 1015, 1995.
[11] R. P. Feynman, "Feynman Lectures on Computation", *Perseus Publishing*, (1st edition). USA, 1999.
[12] C. H. Bennett, "Termodynamics of computation", *International Journal of Theoretical Physics*, vol 21, p 905, 1982
[13] C. H Bennett., G. Brassard, C. Crepeau, r. Jozsa, R., A. Peres and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Phys. Rev. Lett.,* vol 70, p 1895, 1993.
[14] C. H Bennett., G. Brassard, S. Popescu, B. Schumacher, J.A. Solin and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels". *Phys. Rev. Lett, .* vol 76, p 722, 1996.
[15] N. Isailovic, Y. Patel, M. Whitney and J. Kubiatowicz, "Interconnection Networks for Scalable Quantum Computers", *SIGARCH Comput. Archit. News*, vol 34, no. 2, pp 366—377, 2006
[16] A. Kuzmich, W. P. Bowen, A.D. Boozer, A. Boca, C. W. Chou, L.-M Duan, and H.J. Kimble, "Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles", *Nature*, vol 423, p 731, 2003.
[17] C. H van der Wal, M. D. Eisaman, A. Andre, R.L. Walsworth, D.F. Phillips, A.S. Zibrov and M.D. Lukin, "Atomic memory for correlated photon states", *Science,* vol 301, p 196, 2003.
[18] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther and A. Zeilinger, A. "Quantum teleportation across the Danube", *Nature*, vol 430, p 849, 2004.
[19] J.I. Cirac and P. Zoller, "Quantum computation with cold trapped ions", *Phys. Rev. Lett.*, vol 74, p 4091, 1995.
[20] Shnirman, et al. A, "Quantum manipulations of small josephson junctions", *Phys. Rev. Lett*., vol 79, p 2371, 1997.

[21] J.I. Cirac, P. Zoller, H.J. Kimble and H. Mabuchi, “Quantum state transfer and entanglement distribution among distant nodes in a quantum network”, *Phys. Rev. Lett.,* vol 78, p 3221, 1997.

[22] H. Mabuchi, M. Armen, B. Lev, M. Loncar, J. Vu_kovI, H.J. Kimble, J. Preskill, M. L. Roukes and A.Scherer, “Quantum networks based on cavity QED”. *Quantum Information and Computation 1*, Special Issue 7, 2001.

[23] El sitio Web de SETI es *http:// setiathome.ssl.berkeley.edu/*