El rincón de la Ciencia I.S.S.N.: 1579-1149 nº 65 (junio-2013)

Internet cuántica a la vuelta de la esquina (RC-151)

Raúl Issea (Fundación Instituto de Estudios Avanzados – IDEA, Venezuela)

El mundo de la mecánica cuántica (MC) ha trascendido los centros de investigación y universidades hasta formar parte de nuestra cotidianidad. Es frecuente escuchar en las series de televisión como *Stargate SG-1* o *Viaje a las Estrellas* y en múltiples películas hablar de ella, explicando las consecuencias y paradojas de esta ciencia con una familiaridad que muchas veces sorprende.

Hoy en día, se ha corroborado la validez de la MC con datos experimentales. Permítanme recordarles un ejemplo seleccionado al azar cuyo objetivo era establecer la longitud de onda necesaria para que salga un electrón del átomo de helio. Experimentalmente se determinó que dicha longitud de onda de luz debe ser menor a 50.425931 ± 0.000002 nanómetros, mientras que los cálculos mecano-cuánticos predicen una longitud de 50.4259299 nanómetros. ¡Ojalá y no crean que es una coincidencia!

En este trabajo daremos las bases necesarias de la MC para comprender el potencial real de la Internet cuántica, gracias a una serie de experimentos que se comentarán brevemente más adelante, con los que se demuestra cómo la MC está cristalizando cada día más en nuestras vidas.

La moneda cuántica

Imaginemos que tenemos una moneda y deseamos predecir qué lado de ella cae inmediatamente después de lanzarla. Desde el punto de vista clásico, no es posible predecir el resultado porque existe un cincuenta por ciento de probabilidad de que muestre el lado 'cara', y otro cincuenta por ciento de que sea 'cruz'. Si tenemos una moneda cuántica, conocemos que el estado cuántico, el cual abreviaremos como $|\Psi\rangle$, posee toda la información del sistema físico. En este caso, será entonces con la combinación lineal de los estados conformados por los lados de moneda que podremos determinar, bien sea 'cara', abreviemos como $|cara\rangle$, o bien 'cruz', denotado $|cruz\rangle$, con una probabilidad de aparición determinada por los coeficientes α y β, respectivamente. De modo que el sistema que describe nuestro estado será $|\Psi\rangle = \alpha|cara\rangle + \beta|cruz\rangle$, teniendo en cuenta que la moneda no es el estado del sistema, sino $|\Psi\rangle$ donde está presente toda la información del sistema y, por ende, los datos necesarios para resolver el problema.

De modo que si no hemos medido el estado resultante del lanzamiento de la moneda, no podemos inferir un resultado posible, en vista de que el estado del sistema es una superposición de estados infinitos, y solo sabremos qué lado caerá una vez que observemos el lado de la moneda: al verla se determina si es $|cara\rangle$ o $|cruz\rangle$. Esto último no nos sorprende porque tenemos presente que la información del sistema, $|\Psi\rangle$, cambia cuando es observada y mientras eso no ocurre, se tiene una superposición de estados posibles.

De hecho, y empleando el argot de la MC, se puede afirmar que los observables del problema son los dos lados de la moneda (es decir, 'cara' y 'cruz'), que se denominan autovalores del sistema o valores propios, o eigenvalores; mientras que los estados correspondientes son llamados autoestados, estados propios o eigenvectores.

Podemos decir entonces que el problema del lanzamiento de la moneda posee infinitos estados antes de que realicemos la única medida del observable del sistema, cuyos autoestados son 'cara' y 'cruz'. Si uno desea calcular cuánta relación tienen los autoestados entre sí, es decir, y continuando con nuestra notación, determinar el valor de $\langle cara|cruz\rangle$, en nuestro caso será cero porque no es posible tener ambos resultados al mismo tiempo, a menos que la moneda caiga de canto.

¿Por qué Einstein dudaba de la MC?

Los inicios de la teoría de la mecánica cuántica fueron difíciles ya que encontró firmes opositores como Albert Einstein quien dudó de su validez hasta el punto de plantear un experimento teórico con ayuda de otros dos colaboradores. Ellos mostraron una aparente inconsistencia, conocida como la paradoja EPR, iniciales de los autores del trabajo: Einstein, Podolsky y Rosen; que fue publicado en la revista científica *Physical Review* en 1935, con el título "Can Quantum Mechanical Description of Physical Reality Be Considered Complete?" ["¿Puede considerarse completa la descripción de la realidad física de acuerdo a la mecánica cuántica?"]. Cabe resaltar que esta publicación de Einstein fue la más citada en toda su literatura científica.

Paradoja EPR

La paradoja EPR surge para señalar una aparente contradicción que se genera en la MC en vista de que se transmite información más rápido que la luz, es decir, instantáneamente, con independencia de donde estuvieran ubicados los objetos. Einstein, Podolsky y Rosen afirmaban dos hechos cruciales: la no-localidad de la MC (es decir, la posibilidad de una acción a distancia) y el problema de la medición por el hecho de que la MC no permitía realizar predicciones deterministas. Este último comentario establece que tendremos varios resultados posibles de un experimento igualmente posible; lo que conduce a estos científicos a la conclusión de que la MC es

una teoría incompleta.

Más aún, resaltaban que la MC es “incontrolable” durante el proceso de medición, y solamente es posible determinar las probabilidades de obtener un resultado u otro. La sola idea de que la MC presentara una superposición de dos o más estados era imposible de concebir para Albert Einstein.

Este punto es importante porque sin que ellos se lo pudieran imaginar, las consecuencias de sus afirmaciones ayudaron a fortalecer la MC. Nótese entonces que el argumento que sostenía la paradoja de EPR parte del hecho de que se debe cumplir la localidad no predicha por la MC, es decir, los objetos físicos se deberían mover a una velocidad finita y menor a la velocidad de la luz, y debería ser realista la MC, es decir, cualquier objeto debe poseer un estado físico determinado e independientemente de si el mismo es observado o no. Ellos propusieron incluso un concepto llamado elementos de la realidad EPR, es decir, “si, sin perturbar en modo alguno un sistema, podemos predecir con certeza (esto es, con probabilidad igual a uno) el valor de una cantidad física, entonces existe un elemento de realidad física correspondiente a esta cantidad”.

Principio de incertidumbre de Heisenberg

El físico teutón Werner K. Heisenberg mostró a la comunidad científica que es imposible medir simultáneamente la posición y el momento de una partícula, a lo cual denominó el principio de incertidumbre o de indeterminación, formulación que lo hizo acreedor del Premio Nobel de Física en 1932.

Sin embargo, en el año 2012, el equipo de Steinberg de la Universidad de Toronto, en Canadá, realizó un experimento que socavó este principio al enunciar que la medida no es lo que realmente influye en la indeterminación de Heisenberg. Para ello, se concentraron en medir los estados polarizados en los dos ejes que como saben, están estrechamente polarizados. Steinberg nos dice que, efectivamente, no es posible medir los dos estados polarizados al mismo tiempo, pero demuestra que el proceso de medida no incrementa la incertidumbre. Resultado vital a la hora de pensar en la Internet cuántica.

Aporte de John Bell y entrelazamiento cuántico

Fue en 1964 cuando John Bell propuso una forma matemática para reconciliar el mundo de la MC y poder afirmar que esta obedece a leyes deterministas y además se cumple la localidad, gracias a una serie de lo que él denominó desigualdades. La desigualdad de Bell no contradice la paradoja EPR y fue demostrada experimentalmente.

Antes de adentrarnos en esas desigualdades, explicaremos el término entrelazamiento cuántico, el cual proviene de la palabra inglesa *entanglement*, y esta a su vez del alemán *Verschränkung* que usó Schrödinger.

Para comprender el entrecruzamiento cuántico, supongamos que tenemos dos partículas que no están interconectadas físicamente, pero sí correlacionadas entre sí (más adelante explicaremos este último término). De modo que el entrecruzamiento cuántico nos indica que al realizar una medición de una de esas partículas, ya se está condicionando el resultado de la segunda, es decir, que esas partículas comparten una misma existencia.

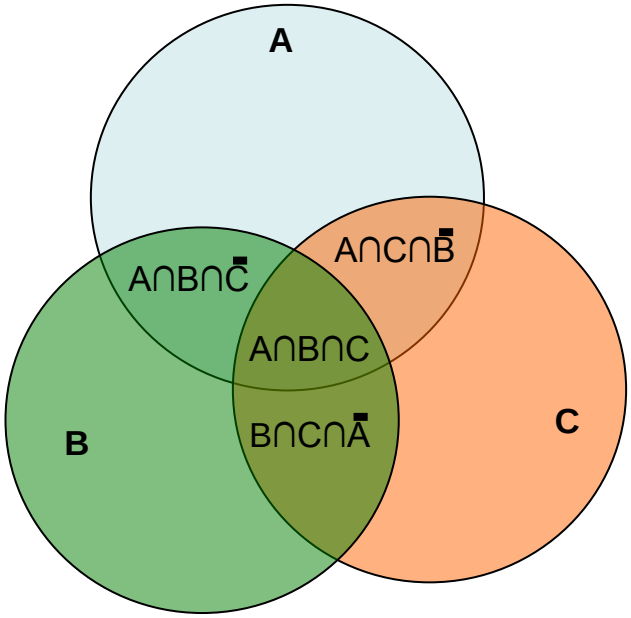
El físico español Guillermo García propone este ejemplo ilustrativo. Tres amigos, Alice, Bob y Carol, participan en el siguiente juego: Carol prepara un rectángulo de papel blanco y un círculo de tela negra. Introduce el primero en un sobre opaco y se lo envía a Alice, y un segundo sobre con el círculo de tela se lo manda a Bob. Ambas cartas están dentro de otro sobre que las cubre para evitar un sesgo en la información. Posteriormente, prepara otro conjunto de sobres, pero esta vez coloca un rectángulo de papel negro y un círculo de tela blanca en cada uno de ellos, y dirige el primero a Alice y el segundo a Bob, y nuevamente los introduce en otro sobre. Repite lo mismo hasta completar ocho parejas de cartas que constituyen una combinación de forma, color y material distintos enviados en pareja a Alice y Bob. Carol mezcla los ocho sobres y selecciona uno (que contiene dos cartas) al azar. Lo abre y envía una carta a Alice y otra a Bob.

Lo sorprendente en términos de la MC es que Alice, al recibir su carta, intenta adivinar su contenido antes de abrirla. Supongamos que adivina su forma, pero no el color ni el tipo de material; predice que recibió un círculo, así que Bob debe haber recibido un rectángulo. Bob hace lo mismo y predice que Alice recibió un círculo. El juego se repite ocho veces y cuando ellos comparan sus resultados, corroboran que hay una correlación perfecta. En el mundo de la MC ocurrirá dicha coincidencia si se pregunta por un único atributo, es decir, solo por la forma (un círculo o un rectángulo), o por el tipo de material (tela o papel) o quizás por el color (blanco o negro).

Explicaremos ahora ese juego, pero en términos de la desigualdad propuesta por John Bell con el siguiente ejemplo. Supongamos que A, B y C son tres propiedades dicotómicas (es decir, admiten solo dos valores posibles, como en lo descrito con Alice y Bob). Si denotamos como N(A,-B) el número de objetos que tiene la propiedad A, pero no presenta la propiedad B, entonces Bell afirmó que $N(A,-B) + N(B,-C) \geq N(A,-C)$; es decir, que el número de elementos del conjunto con la propiedad A, pero que no presentan la propiedad B, más el número de elementos con la propiedad B, pero no la C; debe ser mayor o igual al número de elementos que presentan la propiedad A, pero no la C.

Se puede visualizar lo anterior si empleamos los diagramas de Venn. Recordemos que estos deben su nombre a John Venn, un profesor de Caius College, de la Universidad

de Cambridge, que en 1880 publicó un artículo titulado “De la representación mecánica y diagramática de proposiciones y razonamientos” en la revista *Phylosophical Magazine and Journal of Science*.



En la figura se pueden apreciar las siguientes relaciones:

$N(A,-B) = N(A_o) + N(A \cap C \cap -B)$;
$N(B,-C) = N(B_o) + N(A \cap B \cap -C)$;
$N(A,-C) = N(A_o) + N(A \cap B \cap -C)$;

donde A_o es la parte de A que no está incluida ni en B ni en C (el área de color azul claro), mientras que ∩ simboliza la intersección, y el subrayado superior en la letra es la negación de la propiedad, es decir, $\bar{C}$ es lo mismo que -C. De hecho, si sumamos las dos primeras ecuaciones superiores y restamos la última, se desprende que

$N(A,-B) + N(B,-C) - N(A,-C) =$
$N(A_o) + N(A \cap C \cap -B) + N(B_o) + N(A \cap B \cap -C) - N(A_o) - N(A \cap B \cap -C) = N(B_o) + N(A \cap C \cap -B)$

Obviamente, este resultado mantiene la relación propuesta por Bell por el hecho de que es mayor o igual a cero, lo cual demuestra que $N(A,-B) + N(B,-C) \geq N(A,-C)$. Más aún, podemos seguir validándolo con dos ejemplos adicionales. Pensemos que tenemos N(A,-B, C) + N(-A, B,-C) ≥ 0 en vista de que el número total de objetos es cero; así como el hecho de que N(A,-B,-C) + N(A, B,-C) = N(A,-C).

El aporte de Wehner y Oppenheim en 2010

En el año 2010 se publicó en la revista *Science* un hallazgo inesperado en el mundo de la MC gracias a Jonathan Oppenheim y Stephanie Wehner, de la Universidad de Cambridge y la Universidad Nacional de Singapur, respectivamente, donde mostraban, para sorpresa de todos, que se puede establecer una ecuación científica que relaciona el principio de incertidumbre con la no-localidad, llegando a la conclusión de que la incertidumbre condiciona la cantidad de la no-localidad.

El resultado, irónicamente, es el argumento que emplearon Einstein y sus colegas para socavar la cuántica, y ahora se demuestra que están estrechamente relacionados entre sí. Realmente, ¡la ciencia no deja de asombrarnos!

La no-localidad nos indica "*hasta qué punto dos partes distantes pueden coordinar sus acciones sin tenerse que enviar información entre ellas*", lo que Einstein definía como acción fantasmal a distancia. Para entenderlo, llamemos a Alice y Bob nuevamente, pero ahora Alice creará y codificará la información, y Bob deberá recuperarla, lo cual deberá estar determinado por las relaciones de incertidumbre. Imaginemos un tablero cuántico con solo dos casillas de dos colores diferentes, digamos verde y rojo. Alice coloca una ficha en una casilla de los dos colores y el juego consiste en que Bob adivine en qué color de casilla colocó Alice su ficha, y así ganan el juego, con el pequeño detalle de que los dos están tan separados que no se pueden comunicar físicamente entre sí. Sin embargo, en términos de la mecánica cuántica, ellos siempre van a ganar; posteriormente se darán todos los argumentos para explicarlo.

Gato de Schrödinger

El gato de Schrödinger es la mascota más conocida en el mundo científico producto de un experimento imaginario planteado en 1935 por Erwin Schrödinger. Él planteó una paradoja donde se tenía una caja cerrada que contenía un gato y una botella de veneno que se podía romper a partir de la desintegración de una partícula radioactiva, de modo que existía un cincuenta por ciento de probabilidad de al abrir la caja poder saber si el gato estaba vivo o no. La MC dice que si no se mide, el estado final es la superposición de estados, es decir, el gato está 'vivo' como está 'muerto', y solo abrir la caja condiciona si el gato está vivo o no.

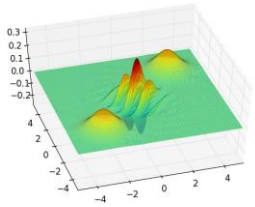
La gata Toti prefiere esquivar cualquier caja que pueda llegar a poner en "duda" su vida.

Al igual que el problema expuesto al principio de este trabajo, este nuevo sistema estará descrito como una superposición de estados 'vivo' o 'muerto' del gato, denotados como $|\psi\rangle = \alpha|vivo\rangle + \beta|muerto\rangle$. Por lo que el estado de vivo o muerto estará correlacionado con la desintegración de la partícula radioactiva o no, respectivamente; y fácilmente se comprenderá que el gato y la partícula radioactiva están enredados cuánticamente.

Igual ocurre con los fotones, las partículas de luz, de modo que al hacer un experimento en óptica cuántica se tendrán dos estados posibles de los fotones implicados en él. Imaginemos que un fotón llega a un cruce, de modo que puede ir a la derecha o a la izquierda. Esto sería erróneo pensarlo porque la MC nos enseñó que el fotón presenta ambas direcciones. Itai Afek y colaboradores, pertenecientes al Instituto Científico Weizmann (Israel), introdujeron los estados NOON en el trabajo que publicaron en 2007, donde se muestra la existencia de los estados NOON de acuerdo a un experimento en óptica cuántica (pero dicho concepto se explicará en otro trabajo).

Decoherencia cuántica

Antes de comenzar a explicar el funcionamiento de la memoria cuántica y la teleportación, factores clave en la Internet cuántica, es importante reseñar un experimento científico realizado en 2008 en el laboratorio Kastler Brosser en CNRS, Francia, mediante el cual se capturó fotográficamente la decoherencia cuántica, es decir, el tránsito de los fotones cuando se pasa de un estado cuántico a otro. Se trata del experimento que permitió fotografiar al gato de Schrödinger en sus dos estados cuánticos.



Resultado obtenido con el programa QuTIP[2] donde se aprecian los dos estados del gato de Schrödinger

Realmente, haber podido registrar la decoherencia cuántica muestra la factibilidad de tener un computador cuántico ya que un estado cuántico entrelazado puede dar lugar a un estado físico clásico. Comencemos entonces a mostrar cada uno de los elementos necesarios para poseer una Internet Cuántica.

Memoria cuántica

Es fundamental destacar el trabajo publicado en 2004 por un grupo de investigadores del Instituto Niels Bohr y el Max Planck donde demostraban que la luz posee en sí misma una memoria cuántica, lo cual haría posible almacenar los impulsos de luz, y lo más importante: que es posible recuperar dicha información con un setenta por ciento de confiabilidad de que haya sido transportada por un vector luminoso.

Este descubrimiento permitió visualizar la existencia de una memoria cuántica denominada qRAM, cuyo análogo clásico es la memoria RAM, gracias al resultado experimental obtenido con un sistema gaseoso de átomos de cesio, donde la información se mantenía por cuatro milisegundos (es decir, el proceso de memoria). Por ello, se puede comenzar a concretar una red formada por computadoras cuánticas donde la información se transmite a través de fotones.

En este punto quizás pueda indicar que cuando almacenamos la información en una memoria cuántica, se debería tener en cuenta que la computadora debe estar aislada para evitar la decoherencia cuántica y que se destruya su estado, en razón de que interactúa con otro sistema que le permite leer o escribir esa información. En tal sentido, los investigadores lograron guardar la información en dos sistemas cuánticos distintos y separados entre sí, uno de los cuales se emplearía para almacenar durante cierto período y otro que fuera de fácil acceso. Esto es posible gracias a que las memorias cuánticas de estado sólido utilizan

el espín nuclear donde están guardados los qubits de forma permanente, y que se acoplan gracias a la interacción hiperfina. Para ello se han empleado átomos de carbono 13 aislados en un diamante de carbono 12 ultrapuro a temperatura ambiente.

Repetidora cuántica

En cualquier red de datos es necesario que se amplifique y replique la información cuando está distribuida, ya que los datos salen del emisor hasta su receptor y se requiere un dispositivo capaz de amplificar los datos, siempre y cuando estén separados por una gran distancia. Dicho dispositivo se llama repetidora cuántica y es otro aspecto esencial de la Internet cuántica. Al igual que la memoria cuántica, el principal reto por vencer en el caso de las repetidoras cuánticas, es que la información debe mantener su naturaleza cuántica.

Para ello, nuevamente el concepto de entrelazamiento cuántico desempeña un rol esencial en las repetidoras cuánticas, teniendo presente el hecho de que dos partículas subatómicas estarán interrelacionadas, en vista de que si una de ellas sufre un cambio de estado, la otra partícula automáticamente reflejará ese cambio en forma instantánea.

Experimento realizado en Tenerife mostrando el poder de la teleportación cuántica. Crédito de la Imagen: IQOQI Vienna/Austrian Academy of Sciences

De hecho, toda repetidora puede ser un *router*, y en ese sentido, se debe mencionar el trabajo de Xiuying Chang y colaboradores, de la Universidad de Tsinghau (China), al construir y probar experimentalmente el primer *router* cuántico de manera que fue posible enviar una superposición de estados mediante el entrecruzamiento cuántico, empleando para ello una información de control que a su vez determina cuál es la que se va a enviar. Advertimos que dicho experimento solo puede enviar un fotón a la vez. Ellos utilizaron dos fotones entrelazados y polarizados, de modo que el *router* funciona usando uno de los fotones polarizados como control, lo cual permite determinar la ruta del otro fotón, justo la señal de datos que se desea transmitir. Recordemos que un *router* normal emplea señales de control que le indican hacia dónde debe enviar la información. A pesar de lo sencillo del experimento, es la primera vez que se visualiza la posibilidad de diseñar y construir e implementar la Internet cuántica.

Teletransporte cuántico vía satélite

La teleportación es un concepto válido en MC, que consiste en transferir un estado cuántico de un lugar sin que físicamente la información cruce un determinado espacio, ya que el mismo se basa en el entrecruzamiento cuántico. Es importante recordar que la teleportación no transporta energía ni masa, solo información.

Aunque este concepto parezca ciencia ficción, el 8 de agosto de 2012 se teletransportó información cuántica sin emplear ningún tipo de cable a través de un recorrido histórico que abarcaba 92 kilómetros de distancia en China, gracias al experimento diseñado por Jian-Wei Pan. Sin embargo, ese triunfo fue rápidamente superado en las Islas Canarias cuando se transportó información a 144 kilómetros. Todo ello revela que el siguiente paso es enviar la información a través de los satélites. No crean que es ciencia ficción, porque Pan y Zeilinger se aliaron para hacer posible la Internet cuántica a través de satélites y se ha pautado para 2016 que China y Europa, así como Norteamérica, lancen un satélite dedicado a realizar experimentos de transferencia de datos a escala cuántica. Se podría afirmar que en 2012 comenzó la carrera espacial cuántica.

Seguridad de la información

Existe una amplia gama de trabajos que muestran las ventajas de la criptografía cuántica. De hecho, la principal ventaja de emplear datos cuánticos es que resulta imposible realizar una copia de la información cuántica al ser uno de los atributos base de la MC, y de esa manera, es posible garantizar que la información no sea alterada. Más aún, es posible detectar rápidamente cuándo se está midiendo dicha información por el hecho de que se genera ruido cuántico introducido por los estados transmitidos. Igualmente importante es que una vez que se realiza la medida cuántica, ella es irreversible. Esta última afirmación se basa en el hecho de que el sistema colapsa a uno de los estados propios del operador correspondiente a la magnitud que se ha medido, y por tanto, siempre habrá una huella/pista de que alguien leyó la información.

En 2008, se implementó por primera vez una transmisión de datos protegida por criptografía cuántica entre doce países. Dicha red está constituida por seis nodos y ocho enlaces ubicados en una distancia que abarca desde los seis hasta los 82 kilómetros, en un anillo de comunicaciones de fibra estándar proporcionada por socios de la SECOQC (siglas en ingles de *Secure Communications based on Quantum Cryptography*); y de esa manera queda demostrado el uso posible de la transmisión de información confidencial. Este esfuerzo implicó cinco años de trabajo y su objetivo fue implementar una criptografía cuántica (en inglés *Quantum Key Distribution,* QKD).

Hackers cuánticos

Después de mostrar cuán segura es la criptografía cuántica, e impulsar el grado de confianza de dicho sistema de seguridad, el equipo de Vadim Makarov, de la Universidad de Noruega, publicó el resultado de un experimento en el que *hackeaban* esa criptografía, es decir, obtenían las claves de encriptación con la ventaja de no dejar ningún rastro en el ataque.

Si nos apoyamos en nuestros amigos teóricos cuánticos Alice y Bob, el equipo de la Universidad de Noruega ideó un método que introduce una "ceguera" momentánea en Alice, de manera que Bob ya no está detectando la señal de ella, y así queda un sistema clásico y no cuántico, haciendo posible obtener las claves de la información.

A pesar de que este procedimiento luce muy sencillo, los equipos para *hackear* información son complicados de manejar, pero lo importante es que Makarov y sus colaboradores lo probaron con dos sistemas de criptografía cuántica comerciales como son el desarrollado por ID Quantique (IDQ), en Suiza, y el sistema de MagiQ Technologies, de Massachusetts.

La concreción de la Internet cuántica está cada vez más cerca; los experimentos que hemos comentado así lo indican. Por ello nos atrevemos a afirmar que está a la vuelta de la esquina, puesto que es posible transmitir a través de satélite los datos que muy probablemente estén encriptados para garantizar su confiabilidad, así como el uso de *routers* y equipos que permiten almacenar la información, porque se ha demostrado que no cambian los datos transmitidos a través de las computadoras cuánticas.