



LAS TIC DEL MAÑANA ¿SERÁN CUÁNTICAS?

Armando López Rodríguez
Ingeniero de telecomunicación
Profesor EOI



Las computadoras cuánticas se basan en las propiedades de la física cuántica, cuyo comportamiento es diferente a las propiedades electrónicas que estamos acostumbrados a encontrar en los equipos de hoy en día, y su unidad básica de información, en lugar de bits, se llama bit cuántico (o qubit). La computación cuántica podría ayudar a identificar, recopilar, traducir y analizar millones de datos en cuestión de segundos, pero aún estamos a las puertas de la revolución digital, pese a todo el camino ya recorrido.

Fue a comienzos de los años 80 del pasado siglo cuando físicos teóricos como los estadounidenses Paul Benioff y Richard Feynman o el israelí David Deutsch apostaban por un cambio de paradigma al proponer aplicar los principios de la física cuántica a los entornos computacionales y tratar de superar así las barreras que ya se vislumbraban en el modelo digital clásico, basado, como sabemos, en el artefacto conceptual ideado por Alan M. Turing en 1936, conocido precisamente como "Máquina universal de Turing".

En las décadas siguientes, varios centros de investigación, destacadas universidades y grandes empresas escrutaron la posibilidad de "cuantizar" varias de las fases del tratamiento de la información según el esquema introducido por Claude E. Shannon y Warren Weaver en su *Teoría matemática de la Comunicación* de 1949 (emisión-codificación-transmisión por canal-decodificación-mensaje). Se pretendía ya alcanzar un modelo de comunicación completo, en este caso cuántico, en el que -mediante la aplicación de las leyes de la mecánica

cuántica y algunos de sus fenómenos característicos- se pudiera mejorar sensiblemente el procesamiento de la información en cada una de las etapas contempladas en la teoría clásica.

Los primeros algoritmos y modelos obtenidos a finales del siglo XX y los inicios del XXI dejaban entrever un potencial considerable cuando pudieran ser aplicados a campos como el de la hipercomputación, la ciberseguridad, la biomedicina o la inteligencia artificial, por ejemplo. El desarrollo experimental de tecnologías basadas

“En los sistemas cuánticos el fenómeno de superposición multiplica exponencialmente la capacidad de realizar operaciones al mismo tiempo”

en las propiedades cuánticas y los sucesivos éxitos en los ensayos de los últimos años han ido corroborando esas expectativas.

Así como en la computación digital clásica la información se codifica por medio de bits, en computación cuántica la unidad básica de almacenamiento de información es el qubit (quantum bit). Pero así como el bit solo puede tomar únicamente dos valores, 0 ó 1, el qubit puede tomar cualquier combinación de sus llamados estados cuánticos básicos, convencionalmente 0^Q y 1^Q , por ejemplo. Es lo que en mecánica cuántica se conoce como superposición de estados. El qubit, por tanto, puede representarse matemáticamente mediante la función de onda:

$$\psi = a \cdot 0^Q + b \cdot 1^Q$$

donde los coeficientes a y b son números complejos que reflejan la probabilidad de que al efectuarse una lectura del estado del qubit se obtenga un 0^Q o un 1^Q , únicos valores posibles debido a que esa acción de lectura sobre el sistema cuántico creado (el qubit) conlleva irremisiblemente el colapso de su superposición.

Si en vez de un qubit pudiéramos tener un sistema de n -qubits, no bastaría con conocer el estado de cada uno de ellos por separado como en los sistemas digitales, pues una posible superposición de los 2^n estados posibles de los n -qubits produciría a su vez nuevos estados. Por esta razón, en los sistemas cuánticos el fenómeno de superposición multiplica exponencialmente la capacidad de realizar operaciones al mismo tiempo.



po en función de los qubits disponibles, lo que significa una indiscutible mayor potencia de cálculo frente a los digitales.

Otra propiedad importante de los sistemas cuánticos es el entrelazamiento, que se define como el estado que se crea bajo determinadas condiciones mediante el cual dos partículas “conectan” sus propiedades caracte-

rísticas, de tal manera que cualquier modificación efectuada en una de ellas es “sentida” por la otra de forma inmediata, por muy distanciadas que se encuentren la una de la otra. Un fenómeno derivado de esta propiedad es el que se ha dado en llamar teleportación, una asombrosa facultad que permite que los sistemas cuánticos puedan ser replicados a una cierta distancia. Si bien replicación en este caso no significaría duplicación, pues la mera interacción al leer el estado para replicarlo ya significaría su destrucción. Es decir, la teleportación cuántica es sólo transporte de información del sistema, no lo es de su materia ni de su energía asociadas.

Como cabía esperar, la posibilidad de conseguir tecnología basada en estas propiedades ha sido todo un reto para diversos equipos de investigadores y la primera teleportación de un fotón conseguida en 1997 y los éxitos de otros ensayos posteriores invitaron a pensar en que su implementación podría dejar de ser ciencia ficción a medio plazo. Hace apenas unos meses logró establecerse por vez primera la complejísima comunicación cuántica entre un satélite chino y una estación terrestre, lo que acerca la posibilidad de llegar a desarrollar a nivel global redes cuánticas de comunicación. El

“Es muy probable que en los próximos años se multipliquen las iniciativas de software cuántico”



“Se investigan diferentes técnicas para tratar de conseguir sistemas estables de varios qubits con interacción continua entre ellos”

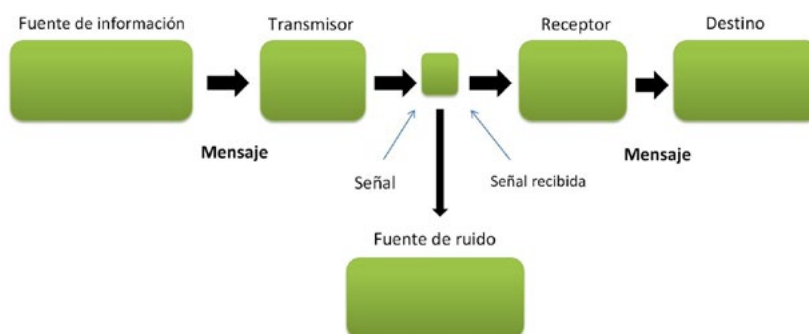
despliegue de este tipo de redes en combinación con el uso de sistemas criptográficos cuánticos, que probablemente se basarían en el Algoritmo de Shor (hasta la fecha el algoritmo cuántico más complejo que aventaja considerablemente en potencia de cifrado a cualquiera de los digitales actuales) permitiría un salto considerable en cuanto al nivel de seguridad e integridad de la información transmitida.

A pesar de las tremendas dificultades para vencer la inestabilidad inherente a los sistemas cuánticos, ya que los estados de superposición y entrelazamiento son extremadamente frágiles y cualquier mínima interac-

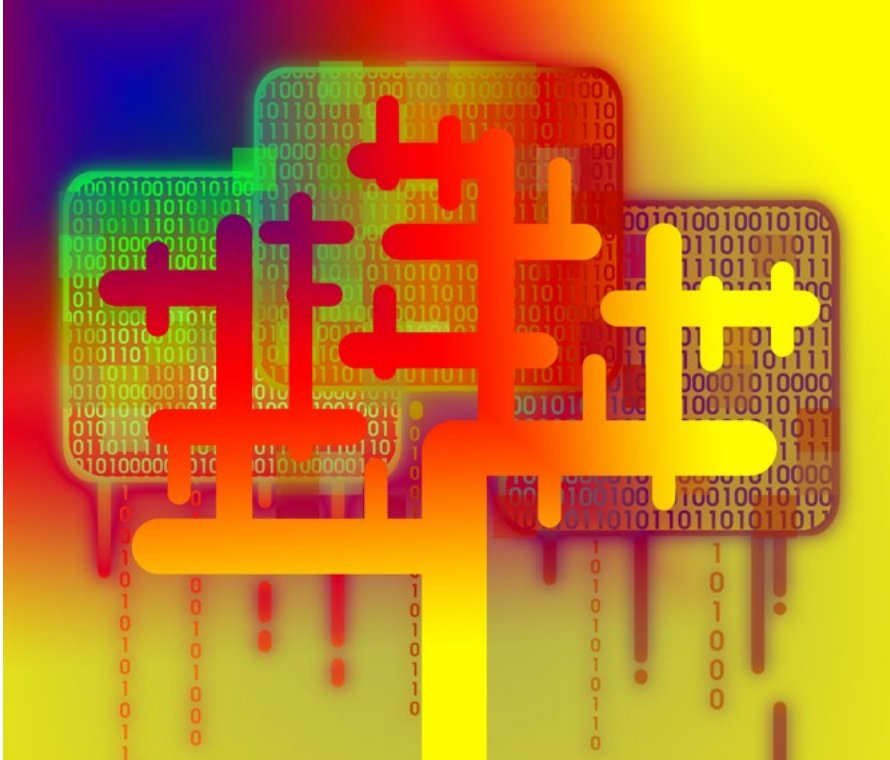
ción con el entorno los colapsa, en los últimos años también se ha asistido a esperanzadores avances en el desarrollo de prototipos computacionales. Las investigaciones se han dirigido al empleo de diferentes técnicas (trampas de iones, materiales superconductores, resonancia magnética nuclear, dispositivos fotónicos, etc.) para tratar de conseguir sistemas estables de varios qubits con interacción continua entre ellos. Pero habilitar las condiciones físicas para mantenerlos es todavía difícil y, por supuesto, muy costoso. A título de ejemplo, las

temperaturas de funcionamiento de algunos entornos no pueden superar apenas el grado centígrado del cero absoluto.

No obstante, aunque diversos laboratorios ya han logrado sintetizar sistemas dotados de varios qubits y puertas lógicas cuánticas, todavía parece lejana una escalabilidad aceptable que les permita competir con los sistemas digitales actuales. Y es que, según comentaba John Martinis, (el físico que lidera el equipo de científicos que Google reclutó en 2014 para



Modelo de comunicación de Shannon y Weaver



hacer posible el primer ordenador cuántico de propósito universal en un plazo estimado no inferior a unas décadas): “Operar incluso un solo qubit es un puzzle de teoría cuántica profunda, física del estado sólido, ciencias de materiales, microfabricación, diseño mecánico y electrónica convencional”.

Pero las investigaciones continúan, y a pesar de las enormes inversiones necesarias instituciones de diferentes países y gigantes de la informática como Microsoft, IBM, Intel o el citado Google, han demostrado estar apostando fuertemente por esta tecnología. IBM, por ejemplo, ha

puesto en la nube un prototipo de ordenador cuántico de cinco qubits para que ingenieros e investigadores en general lo testeen y puedan probar en él algoritmos y pequeñas programaciones cuánticas. Y ha anunciado su intención de irlo sustituyendo paulatinamente por modelos de decenas de qubits. Es indudable que la oportunidad de operar con esos prototipos experimentales para muchos supondrá todo un desafío, por lo que es muy probable en los próximos años se multipliquen las iniciativas de desarrollo de software cuántico.

La NASA y otras potentes corporaciones no han dudado en desem-

bolsar los alrededor de 10 millones de dólares que cuesta uno de los modelos que la canadiense D-Wave comercializa desde 2011 como los primeros ordenadores cuánticos del mundo. El más moderno, aparecido a comienzos de este mismo año, dispone según su fabricante de un procesador de 2000 qubits. No se trata de un ordenador cuántico puro (el denominado topológico). Está basado en superconductores y en su núcleo de qubits no se producen estados de entrelazamiento, por ejemplo. A la vuelta de la esquina están también los basados en semiconductores, tampoco estrictamente cuánticos, pero capaces de sacar partido del potencial de algunos de los comentados efectos de la física cuántica.

Sin embargo, parece que todavía nos encontramos a unas décadas de poder ver el realmente anhelado por los investigadores: un computador cuántico puro, topológico, capaz de competir con los hipercomputadores digitales a un coste razonable. Todavía más remoto parece su uso doméstico, si es que llega a producirse algún día. Lo más probable, por tanto, es que asistamos, al menos en un principio, a una convivencia con la robusta tecnología digital clásica, aunque sin descartar tampoco otras igualmente en vías de investigación, como la basada en ADN, por ejemplo.

Aunque, sobre lo que vaya a ocurrir en el mundo tecnológico del mañana, como dice el cantante: “¿qué sabe nadie?” Han sido ya tantos los vaticinios luego absolutamente pulverizados...

Tomorrow's ICT, will they be quantum operations?

Quantum computing is a computing paradigm different from that of classic computing. It is based on the use of qubits instead of bits, and opens new

logic gates that make new algorithms possible. This type of technology allows doing various complex tasks simultaneously, so that multitudes of processes

are sped up exponentially. It is still to be seen if the future of the ICT passes through quantum computing, since there is still a long way to go.