Cómputo Cuántico y su Desarrollo Actual

José Ruiz-Ayala[1]
Tecnológico Nacional de México /
Instituto Tecnológico de la Laguna
Blvd..Revolución y Calz. Tecnológico S/N
Torreón, Coah.. México, C.P. 27000
jdruiza@lalaguna.tecnm.mx

Ruth de la Peña - Martínez[2]
Tecnológico Nacional de México /
Instituto Tecnológico de la Laguna
Blvd. Revolución y Calz. Tecnológico S/N
Torreón, Coah.. México, C.P. 27000
rdelapenam@lalaguna.tecnm.mx

Resumen: El propósito del presente estudio, es revisar el estado actual del desarrollo del cómputo cuántico en general, y particularmente en México. El principal problema que se presentó es el alto costo de los productos o prototipos que ya existen en el mercado, invertir USD $ 10,000,000 no es algo sencillo; nos limitamos a las opiniones de los fabricantes como D-Wave e IBM, pero para equilibrar la opinión de dos proveedores, se hizo un recorrido sobre el tema, recabando información de expertos en el tema, incluso detractores sobre este tópico, e incluyendo algunas opiniones de quienes han invertido en esta tecnología. Los resultados son complicados de asimilar, porque no solo es pensar en tener los recursos para invertir, sino que es toda una tecnología que requiere profundos conocimientos de la física y la mecánica cuánticas, la ventaja es que hay tiempo para ir tomando cartas en el asunto. Un hallazgo importante es el hecho de que sí se están haciendo esfuerzos en México, y otro es que el riesgo de la seguridad ante estos nuevos equipos, no es cómo algunos autores han planteado, habrá soluciones acordes con la situación. Se concluye que, aunque los primeros prototipos de tuvieron desde 2010, es una tecnología todavía en desarrollo, y que van a pasar años para que sea de uso generalizado, tiempo en el cuál las instituciones de educación superior podrán ir capacitando a sus plantas docentes de Tecnologías de Información.

Palabras Clave: Cómputo Cuántico, Criptografía Cuántica, Algoritmos Cuánticos.

Abstract: The purpose of this study is to review the current state of quantum computing development in general, and particularly in Mexico. The main problem that was presented is the high cost of products or prototypes that already exist in the market; investing USD $10,000,000 is not easy; we limited ourselves to the opinions of manufacturers such as D-Wave and IBM, but to balance the opinion of two suppliers, a review was made on the subject, gathering information from experts on the subject, including detractors on this topic, and including some opinions of those who have invested in this technology. The results are difficult to assimilate, because it is not

only about having the resources to invest, but it is a whole technology that requires deep knowledge of physics and quantum mechanics; the advantage is that there is time to take action on the matter. An important finding is the fact that efforts are being made in Mexico, and another is that the security risk with these new devices is not as some authors have suggested, there will be solutions in accordance with the situation. It is concluded that, although the first prototypes were created in 2010, it is a technology still in development, and that it will take years for it to be in widespread use, during which time higher education institutions will be able to train their teaching staff in Information Technology.

Key words: Quantum Computing, Quantum Cryptography, Quantum Algorithms.

Introducción

Desde mediados del siglo pasado, y principalmente a partir de los años 80´s, con la aparición de las microcomputadoras, ha habido una especie de revolución en el campo de las Tecnologías de Información y Comunicaciones (TIC), apareciendo una gran cantidad de productos o desarrollos a la medida, para resolver todo tipo de problema. Eso ha generado una espiral creciente de mayores requerimientos en la capacidad de cómputo. Ese aspecto ha sido apoyado por el gran desarrollo tecnológico en la miniaturización de los microprocesadores, pero eso parece tender a llegar a su límite.

Hace cuatro décadas toma forma la aplicación de teorías cuánticas, en la construcción de compuertas electrónicas, que además de procesar información mucho más rápido, permita aplicar algoritmos más avanzados que no se pueden implementar en una computadora convencional. Los prototipos que se han construido hasta hoy en día, han dado solución a problemas muy específicos, pero están lejos de ser una computadora de uso general, otros aspectos son su sensibilidad al medio ambiente, ruidos eléctricos, magnéticos, o ambientales. Pero el problema central es su costo, si no llega a ser posible construir un equipo cuántico a un costo asequible para las empresas o instituciones, no entrará en auge esta tecnología.

De cualquier manera, hay que ir dándole seguimiento al desarrollo cuántico, para preparar en la medida de lo posible a las generaciones futuras, que seguramente verán florecer este tipo de computadoras. Revisaremos algunos conceptos básicos para tener una idea de la arquitectura cuántica, e imaginar cuán potente puede llegar a ser. Luego veremos a grandes rasgos la evolución tanto de los equipos de D-Wave como de IBM, para evaluar que logros han tenido, los retos que enfrentan, al menos saber qué y quienes están trabajando en esta tecnología, en el ámbito internacional y finalmente en México.

Cabe aclarar como parte del mencionado seguimiento a esa tecnología, como siempre, tenemos la parte de software y la de hardware, que van y seguirán de la mano. Se incluyen las opiniones de algunos críticos, como parte del análisis de la situación, pero en opinión de quienes esto escriben, así como en 1945 solo se tenía una gran computadora en IBM, y que no se pensaba que pudiera haber más de cinco de ellas en el mundo, cambiando todo a partir de 1980, cuando vino el boom de las microcomputadoras y de servidores de buena capacidad y accesibles en precio, llegará el tiempo de que nuestras portátiles y computadoras de escritorio, sean computadoras cuánticas. De inicio, en 2023 la Universidad Nacional Autónoma de México (UNAM), adquirió dos computadoras cuánticas para la Facultad de Ingeniería, a la cual le acondicionaron acceso remoto, para estudiantes y profesores (Milenio, 2023).

Si bien el cómputo cuántico es un cambio paradigmático más grande que cuando pasamos de la programación funcional a la programación en objetos, hay que considerar que bajo la óptica de la compañía D-Wave, una computadora cuántica (CC) opera bajo las órdenes de una consola que es una computadora convencional, donde tenemos lenguajes como C++, Java y Python, por el lado de la programación quedan por aprender o conocer los algoritmos cuánticos ya desarrollados. Esto sería muy transparente, pero no así en el caso del hardware, que empezando con el hecho de que requiere las condiciones para operar cerca de los cero ^{o}K, para aprovechar las propiedades de los superconductores, no va a ser fácil tener un equipo portátil en esas condiciones.

Se agrega la sección de los críticos o detractores, para enfatizar los retos que se han tenido o que todavía se tienen, de tal suerte que esta tecnología sigue en desarrollo. Se hace hincapié en el hecho de que las CC actuales son de uso específico, para entender sí las críticas son legítimas, y demeritan a los equipos en funciones, o simplemente su diseño no contempla lo que se señala, aspecto que de antemano se sabe deberá quedar resuelto cuando ya tengamos CC de uso general.

Metodología.

Se aplicó un método cualitativo, para conocer el estado del arte en el desarrollo del cómputo cuántico. Por medio de la Investigación descriptiva, se analizó el contexto internacional y nacional, sobre los elementos básicos del software y hardware cuánticos, para contextualizar la investigación. La técnica de recolección y análisis de datos cualitativos fue la revisión de material de bibliografías, documentos y registros, analizando los datos a través de organización y

transcripción de material, utilizando bitácoras para documentar el proceso, dando como resultado un panorama respecto a los sucesos de las computadoras cuánticas.

Fundamentos de las computadoras cuánticas (CC).

Primero veamos la diferencia básica de un bit que puede tomar dos valores, cero o uno, esto en la computación convencional. En las CC el equivalente al bit es el cúbit o bit cuántico, que es un vector tridimensional, con diferentes magnitudes y diferentes direcciones, representando ceros y unos para cada octante (Figura 1.). Luego empiezan las grandes diferencias con las propiedades de los cúbits (Nowak, 2024):

(a) Superposición. Significa que un cúbit pueda estar en varios estados al mismo tiempo, como si un bit convencional estuviera en cualquier lugar de la esfera de Bloch o bit cuántico. Esta propiedad es la que utiliza el CC para evaluar o procesar al mismo tiempo cada una de las posibles combinaciones de todos los cúbits, dando como resultado un aumento exponencial en la potencia de cálculo para problemas de algún tipo específico.

(b) Entrelazamiento o entramado. Se presenta al relacionar dos o más cúbits, dando como resultado que el estado de uno depende del otro. Así es como un CC procesa cúbits de manera agrupada y coordinadamente, aspecto esencial en el manejo de algoritmos cuánticos. Una aplicación de esto es la criptografía cuántica, ya que al medir un cúbit asociado, se altera el estado del otro, revelando la interferencia.

(c) Interferencia. Proceso que refuerza o cancela estados de los cúbits entre ellos, esto se usa para orientar un algoritmo a la respuesta correcta, eliminando estados que lo conducen a soluciones incorrectas.

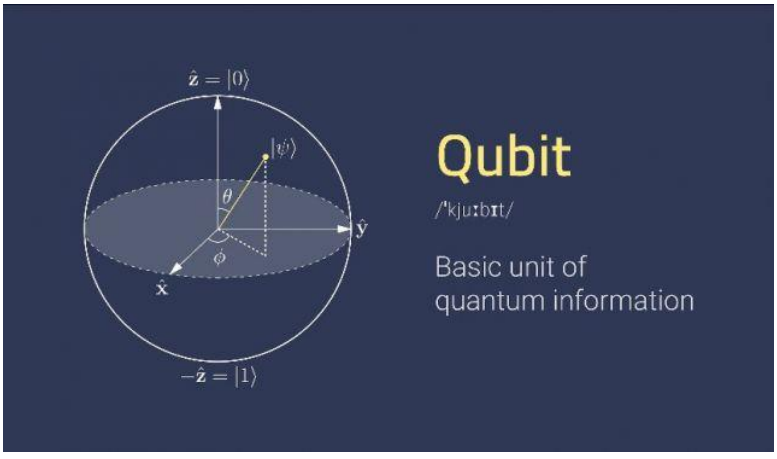

Figura 1. Bit cuántico.
Nota: Obtenido de (TSTC en Vivo, 2024)

(d) Recocido (quantum annealing). Los sistemas D-Wave utilizan este en la búsqueda de soluciones a un problema. Se basa en la tendencia natural del mundo cuántico que busca estados de baja energía. El cálculo empieza poniendo la unidad de procesamiento cuántico (QPU por sus siglas en inglés) en un estado determinado a un problema conocido, aplicando el proceso de quantum annealing, se solucionará el problema de modo que se mantenga un estado de baja energía durante todo el proceso. Al final del cálculo, cada qubit termina como 0 o 1. Este estado representa la solución óptima o casi óptima al problema.

En la naturaleza, los sistemas físicos tienden a cambiar hacia un estado de energía más baja: los objetos se deslizan cuesta abajo, las cosas calientes tienden a enfriarse y así sucesivamente. Este comportamiento es la premisa que determina el comportamiento de los sistemas cuánticos. Una analogía, es imaginar un viajero que busca como la mejor solución, encontrar el valle más bajo en el paisaje energético que representa el problema. Los algoritmos típicos buscan el valle más bajo poniendo al viajero en algún punto del entorno y dejan al viajero moverse localmente. Por lo regular es más eficiente ir cuesta abajo y evitar subir colinas altas, en estos algoritmos clásicos es común llevar al viajero a valles cercanos que tal vez no sean el mínimo de todo el contexto. Por medio de muchos ensayos, con muchos viajeros que comienzan sus viajes desde diferentes puntos.

En cambio, el quantum annealing da inicio con el viajero colocado al mismo tiempo en muchas coordenadas usando al fenómeno cuántico de la superposición. La probabilidad de estar en cualquier coordenada determinada avanza suavemente con el progreso del método, con esto tiene la probabilidad de aumentar su cercanía alrededor de los valles profundos. La Tunelización cuántica permite al viajero pasar por las colinas, en lugar de tener que escalarlas, lo que minimiza la posibilidad de quedarse atrapado en valles que no son el mínimo contextual. El entrelazamiento cuántico mejora aún más el proceso dejando al viajero encontrar relaciones entre los puntos que conducen a valles profundos.

Pasar de un solo cúbit a un QPU multi- cúbit requiere que los cúbit estén interconectados para intercambiar información. Los cúbit se conectan mediante acopladores, que también son bucles superconductores. La interconexión de cúbits y acopladores, junto con los circuitos de control para gestionar los campos magnéticos, crea un tejido de dispositivos cuánticos programables. Cuando la QPU llega a una solución de un problema, todos los cúbits se asientan en sus estados finales y los valores que retienen se devuelven al usuario como una cadena de bits. Por ejemplo, el sistema D-Wave 2000Q tiene hasta 2048 cúbits y 6016 acopladores. Para alcanzar esta escala,

utiliza 128,000 uniones Josephson, lo que hace que este computador sea, con mucho, el circuito integrado superconductor más complejo jamás construido (Figuras 2 y 3) (D-Wave, 2018).

Figura 2. CC D-Wave modelo Quantum 512.
Nota: Obtenido de (D-Wave, 2018)

Figura 3. Procesador Quántico.
Nota: Obtenido de (D-Wave, 2018)

Sobre las uniones Josephson, están compuestas por un par de superconductores, separados por un aislante muy delgado. De tal forma que pueden transitar por dicha unión, pares de electrones prácticamente sin resistencia, fenómeno conocido como túnel cuántico. Es así como disponiendo

los superconductores bastante cercanos, se permite que pasen por la barrera que los aísla, pares de electrones que generan una corriente eléctrica sin pérdida de energía (Modern Physics, 2024).

Empresas que están impulsando la tecnología de CC.

Primero veamos algunos detalles adicionales a la ya mencionada D-Wave y luego otras como IBM, IonQ, Quantinuum, Atom Computing y Quera (Millán, 2023).

(a) D-Wave. En 2010 vendió sus primeras computadoras de 512 cúbits a la NASA, Lockheed Martin, Google, Volkswagen, entre otros. Este año anunció su prototipo Advantage2 con 1,200 cúbits, y el doble de acopladores que su versión anterior, con lo que se espera un rendimiento del 20% más que la Advantage1 (DCD, 2024).

(b) IBM Quantum. En su hoja de ruta marca 2033 como el año en que lanzará su primer CC de propósito general. A la fecha ha ofrecido soluciones para el sector farmacéutico, Química, e Inteligencia Artificial, específicamente en Aprendizaje Máquina o Machine Learning. La plataforma de desarrollo de software es el Quantum Qiskit, que es una plataforma de pila completa Figura 4 (Schneider & Smalley, 2024).

(c) IonQ. Empresa muy fuerte en la comercialización, después de firmar contratos con AWS de Amazon, y Azure de Microsoft, cotiza en la bolsa de valores de New York.

(d) Quantinuum. Producto de la fusión de la empresa Honeywell y un equipo universitario, el Cambridge Quantum Computing en el año de 2021. Si bien solo cuenta con 450 empleados, su modelo H2, basado en trampa de iones, tiene una capacidad de 32 cúbits.

(e) Google. Con su modelo Quantum AI, está dirigido al desarrollo de hardware y software pensados para una computadora de uso general, ofrece una solución de pila completa tanto en software como en hardware (Google, 2024).

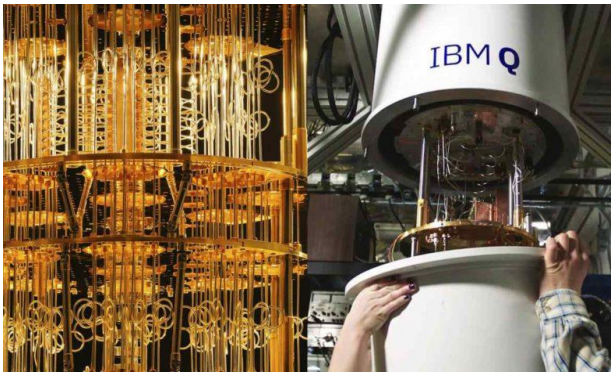

Figura 4. La IBM Quantum.
Nota: Obtenido de (Schneider & Smalley, 2024)

Desafíos del cómputo cuántico.

Como ya se mencionó, hay muchas CC de fines específicos, pero todavía hay bastantes cuestiones que resolver, veamos las más destacadas:

(a) Errores y limitaciones de rendimiento. Como ya se comentó, una CC es muy sensible a cualquier ruido como campos magnéticos, señales de transmisión de comunicaciones, variaciones atmosféricas inclusive. Aunque es el motivo porque se colocan dentro de contenedores que aíslan precisamente ese tipo de factores, de pronto aparecen errores, es probable que dependan de comportamientos erráticos en algún componente, o alguna otra cuestión técnica en el procesador, las compuertas, los acopladores, etc. EL hecho es que esta situación requiere solución, CC libres de errores (Amin, 2015).

(b) Comparación con computadoras cuánticas universales. La mayoría de los modelos son de uso específico, siendo entonces crucial la construcción de equipos de uso general en cualquier marca (King, Raymond, Lanting, Isakov, & Mohseni, 2021).

(c) Competencia de supercomputadoras clásicas. Se ha demostrado que en muchas situaciones las computadoras clásicas han tenido un mejor desempeño al ser más rápidas que alguna CC con la que se haya comparado. Esto produce incertidumbre en el tan esperado mejoramiento espectacular en el rendimiento (McGeoch, 2014).

Características principales de la empresa líder D-Wave.

(a) Enfoque en problemas de optimización. Su diseño está dirigido a la solución de problemas de combinatoria y búsqueda en grandes cantidades de datos, así como su aplicación en logística en la determinación de rutas, problemas financieros y modelado de materiales. Industrialmente hablamos de aeronáutica, automoción y energía.

(b) Comercialización temprana. Como pionero en este tópico, en sus desarrollos específicos para la Volkswagen, Lockheed Martín y la Nasa, logró consolidarse como desarrollador senior en CC.

(c) Accesibilidad a su tecnología. A cambio de lo costoso de sus equipos, el proporcionar laboratorios virtuales, dio acceso a las empresas interesadas y a investigadores de cualquier sector, a construir soluciones cuánticas y probarlas sin tener que comprar el equipo, solo para efectos de evaluación (D-Wave, 2018). Sin embargo, analicemos lo expresado por (Dargan, 2023) y por su parte (Law, 2023), ya que como vemos en la Tabla 1, no aparece D-Wave:

D-Wave es una de las primeras empresas en comercializar computadoras cuánticas, pero su tecnología se basa en un enfoque específico conocido como quantum annealing o recocido cuántico, que es más adecuado para resolver problemas de optimización que para ejecutar algoritmos cuánticos generales como los de IBM o Google. D-Wave ha sido muy relevante en el campo de la computación cuántica desde su fundación, y ha vendido más de 30 sistemas a diferentes instituciones y empresas.

Pero en el contexto reciente de los *jugadores más importantes*, su tecnología (de D-Wave) ha sido algo eclipsada por otras plataformas que utilizan cúbits superconductores o cúbits atrapados, que son más versátiles para el desarrollo de computadoras cuánticas generales. En resumen, mientras D-Wave sigue siendo un actor importante, su nicho especializado en quantum annealing no le permite competir directamente en el mismo campo que las empresas que están desarrollando computadoras cuánticas universales.

Tabla 1. Cinco principales proveedores de computadoras cuánticas, basados en su liderazgo tecnológico y ventas recientes

Proveedor	Ingresos $USD Aproximados últimos 5 años	Cantidad de equipos	Descripción Breve
IBM	Más de $500 millones	Al menos 20 grandes sistemas cuánticos	IBM es líder en el campo, con el lanzamiento de su sistema IBM Quantum One en 2019 y avances como su chip Condor de 1,000 cúbits. Sus planes para 2025 incluyen el desarrollo de sistemas modulares
Google (Alphabet)	Aproximadamente $200 millones	Desconocido	Google Quantum AI ha sido pionero en la creación de procesadores cuánticos y en la investigación de algoritmos de corrección de errores, con el objetivo de construir una computadora cuántica a gran escala
Amazon (AWS Braket)	Más de $100 millones	Acceso en la nube a múltiples sistemas	Amazon ofrece su servicio Braket, que proporciona acceso en la nube a varias plataformas cuánticas, lo que ha democratizado el uso de estas tecnologías
Microsoft	Más de $100 millones	Desconocido	Microsoft está desarrollando su propia computadora cuántica basada en cúbits topológicos y ofrece acceso a sus tecnologías a través de Azure Quantum
Alibaba	Desconocido	Al menos 2 grandes sistemas cuánticos	Alibaba, a través de su Quantum Lab en China, está trabajando en tecnologías superconductoras para computadoras cuánticas

Fuente: (Dargan, 2023; Law, 2023)

Detractores de las CC.

Gil Kalai hace énfasis en el problema de la Decoherencia, que a grandes rasgos es la pérdida de la asociación de dos o más cúbits, perdiendo su propiedad cuántica y exhibiéndose como un bit cuántico convencional, una verdadera tragedia, pero que llega a pasar (Stankevich & Studenikin, 2019). Susskind (2018) más que nada hace una crítica constructiva de los riesgos y dificultades que se presentan en las CC, y los engloba en lo mismo, que no hay mayor rendimiento comparado con el costo, y que hay errores (Susskind, 2018).

Un trabajo sobre análisis de la velocidad de las CC, examina cómo se puede definir y medir la velocidad cuántica, demostrando que muchos de los problemas abordados por D-Wave no necesariamente muestran ventajas cuánticas claras sobre los métodos clásicos (Ronnow, Wang, & Troyer, 2014). Aaronson ha sido crítico del enfoque de D-Wave desde sus primeros días, argumentando que el recocido cuántico no representa un avance significativo en comparación con las técnicas clásicas para ciertos tipos de problemas. Aunque reconoce que D-Wave tiene potencial en algunos casos específicos, ha expresado escepticismo sobre si sus máquinas pueden escalar para resolver problemas de manera más eficiente que los sistemas clásicos (Aaronson, 2015).

Criptografía cuántica.

Es cierto que el desarrollo teórico de la criptografía cuántica ha avanzado más rápidamente que el desarrollo real de las CC. La criptografía cuántica, en particular las técnicas como la distribución de claves cuánticas (QKD, Quantum Key Distribution), ya ha demostrado ser viable en entornos experimentales y comerciales. Estas técnicas ofrecen seguridad basada en principios fundamentales de la física cuántica, lo que hace que sea prácticamente imposible interceptar una clave sin que el emisor o receptor lo detecten (Scarani & Kurtsiefer, 2014). El concepto de distribución de claves cuánticas (QKD) es uno de los avances teóricos más importantes en criptografía cuántica. QKD permite que dos partes compartan una clave secreta de manera segura utilizando las propiedades de la mecánica cuántica, específicamente el principio de superposición y el de entrelazamiento cuántico. Desde 2019, varios estudios y proyectos han demostrado que QKD puede implementarse sobre redes ópticas actuales, como las fibras ópticas e incluso a través de satélites. A pesar de esto, su uso a gran escala aún está limitado por factores prácticos como la distancia y la velocidad de transmisión (Law, 2023).

Las computadoras cuánticas, están avanzando lentamente. Aunque empresas como IBM y Google han hecho progresos significativos, el escalado a sistemas grandes y estables que

puedan superar las capacidades de las computadoras clásicas sigue siendo un desafío. El error de los cúbits y la dificultad para mantener estados cuánticos estables por períodos prolongados limitan su desarrollo práctico, y las computadoras cuánticas actuales solo funcionan bien para casos específicos y pequeños Figura 5 (Yin, Li, & Liao, 2020).

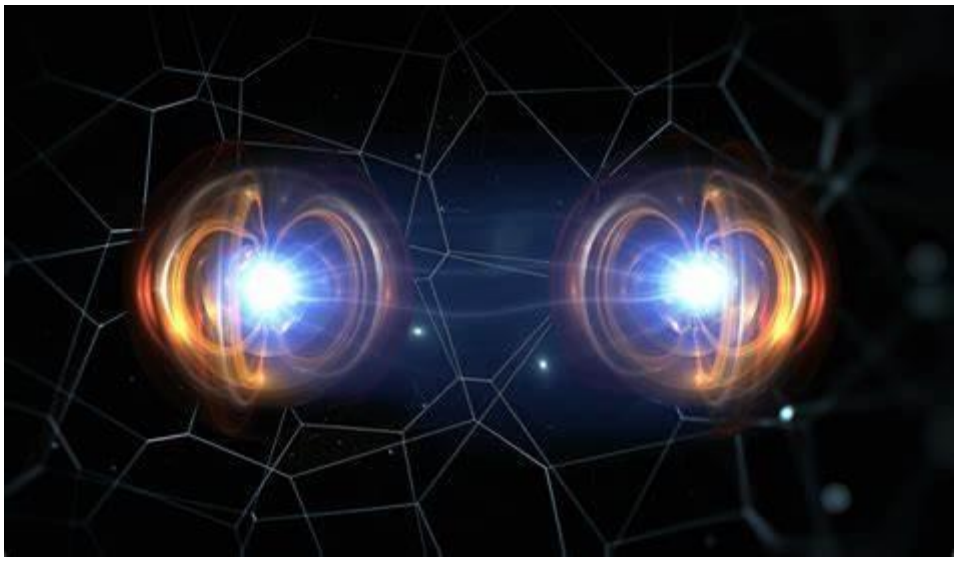

Figura 5. Criptografía Cuántica.
Nota: Obtenido de (Carpineti, 2020).

Los sistemas de cifrado simétrico, como el Estándar de Encriptado Avanzado (AES por sus siglas en inglés), son más resistentes a los ataques cuánticos directos mediante fuerza bruta. El algoritmo de Grover, que es el análogo cuántico a la búsqueda por fuerza bruta, solo ofrece una mejora cuadrática (es decir, reduce el tiempo de búsqueda de (N) a (√N). Esto significa que, aunque la computación cuántica puede acelerar la búsqueda, no sería suficiente para romper de manera práctica cifrados simétricos fuertes, como el AES-256, sin un número masivo de cúbits.

El hecho de que las computadoras cuánticas puedan eventualmente acelerar los cálculos combinatorios, y potencialmente realizar búsquedas exhaustivas mucho más rápido que las computadoras clásicas, es una preocupación legítima. Si las computadoras cuánticas logran superar las limitaciones actuales y llegar a la escala suficiente, podrían romper ciertos cifrados mediante la fuerza bruta. Sin embargo, en la práctica actual, no tenemos computadoras cuánticas suficientemente potentes para ejecutar estos ataques. Los sistemas cuánticos actuales están limitados por la cantidad de cúbits y los errores de decoherencia. Aunque el algoritmo de Shor podría romper algoritmos de llave pública como RSA (Acrónimo de Rivest, Shamir y Adleman), o el de Criptografía de Curva Elíptica (ECC por sus siglas en inglés), necesitaría millones de cúbits

estables para ejecutar estos ataques a gran escala, algo que está muy lejos de las capacidades actuales.

La criptografía post - cuántica está avanzando rápidamente, lo que significa que, para cuando las computadoras cuánticas sean una amenaza real, ya podrían estar disponibles soluciones criptográficas que mitiguen este riesgo. En resumen, mientras las computadoras cuánticas representan una amenaza teórica a largo plazo, en la actualidad aún no tienen la capacidad de romper los cifrados clásicos en un tiempo razonable mediante fuerza bruta. Sin embargo, es crucial que sigan los esfuerzos en la investigación de criptografía resistente a ataques cuánticos para estar preparados para ese futuro (Amit, Shabtai, & Elovici, 2024).

Resultados

Después de la aparición de la computadora D-Wave One en 2010, se pensó que las CC finalmente entraban en escena, sí y no. Sí porque finalmente se ponía en práctica una computadora con bits y compuertas cuánticas, que permitían aplicar algoritmos cuánticos que no se podían procesar en computadoras convencionales. Rápidamente se detectaron dos problemas, su costo del orden de $ USD 10,000,000 y la otra que era de fines muy específicos, como aplicaciones de la combinatoria.

La evolución ha continuado, con muchas esperanzas cifradas en los prototipos de IBM que van encaminados a CC de uso general, la situación es que en cualquier caso se siguen tratando de resolver errores en la ejecución, que computacionalmente no son aceptables. Hay una propuesta muy interesante, pero sigue en etapa experimental, que son las trampas de iones o iones atrapados, que representan cúbits más estables por mayor tiempo, y se espera que se logre con ellos la solución a los errores presentados.

Es tranquilizante saber, que lo que se vislumbra en un corto plazo, es que realmente las CC no representan un problema para los sistemas de criptografía actuales. En adición a esto, previendo un mayor y más rápido desarrollo tecnológico de las CC, paralelamente y de tiempo anterior, se está trabajando en algoritmos de cifrado cuántico, y que se prevé que estarán a la altura llegado el momento.

Hallazgos y/o conclusiones

El primer aspecto a resaltar es que la aparición en el mercado de las CC de D-wave desató el interés por esta tecnología, llevando a otras empresas a incursionar en este segmento del mercado. Esto ha repercutido en los gobiernos, en nuestro caso en México y las Instituciones

Educativas, aspecto esencial, porque este nuevo paradigma, implica especialización de quienes programarán las CC, que requieren conocimientos de física, matemáticas y mecánica cuánticas.

Una grata sorpresa es la adquisición de dos computadoras por la Universidad Nacional de México (UNAM) el año pasado. Este año es probable entonces, que el Instituto Politécnico Nacional (IPN) también adquiera al menos una. Para el sistema del Tecnológico Nacional de México no tenemos noticias, pero esperemos se tengan los recursos para incursionar también en las CC.

Por las proyecciones de las empresas consideradas, se espera para finales de esta década y principios de la siguiente, ya entrar más de lleno a las Tecnología de Información (TI) en equipos cuánticos, primero menos costosos, que cumplan las expectativas de rendimiento y de uso general, y claro confiables, libres de errores. Lo cual nos lleva a incursionar en la investigación de varias especialidades con el apoyo de las tecnologías. A lo anterior agregamos que ya las TI están sometidas a un desarrollo intenso, constante, y muy variado, en todas las áreas de software y hardware, y sub – áreas como Desarrollo Web, Cómputo en la Nube, Big Data, Inteligencia Artificial entre otras.

Resulta entonces prácticamente una revolución tecnológica, mover las TI a un entorno cuántico, con nuevos equipos, nuevas aplicaciones y nuevas estrategias de negocios, porque la visión es que todo va a funcionar de manera más eficiente, pero a un costo mayor, y con una necesidad imperiosa del conocimiento de las bases y todo el soporte de un mundo de TI en el contexto cuántico.

Referencias

Aaronson, S. (15 de enero de 2015). *CERN. Quantum Computing and the Limits of the Efficiently Computable.* Obtenido de https://cds.cern.ch/record/1981892

Amin, M. (19 de noviembre de 2015). *Physical Review. Searching for quantum speedup in quasistatic quantum annealers.* doi:10.1103/PhysRevA.92.042303

Amit, G., Shabtai, A., & Elovici, Y. (2024). *IEEE. A Self-Healing Mechanism for Internet of Things Devices.* Obtenido de https://ieeexplore.ieee.org/document/9187198

Carpineti, A. (22 de diciembre de 2020). *Technology. New Quantum Computing Method Entangles Photons 100 Times More Efficiently Than Before.* Obtenido de https://www.iflscience.com/new-quantum-computing-method-entangles-photons-100-times-more-efficiently-than-before-58130

Dargan, J. (29 de diciembre de 2023). *The Quantum Insider. Quantum Computing Companies: A Full 2024 List.* Obtenido de https://thequantuminsider.com/2023/12/29/quantum-computing-companies/

DCD. (25 de enero de 2024). *Datacenter Dynamics. D-Wave anuncia computadora cuántica de 1.200 qubits.* Obtenido de https://www.datacenterdynamics.com/es/noticias/d-wave-anuncia-computadora-cuantica-de-1200-qubits/

D-Wave. (25 de Enero de 2018). *D-Wave Systems Inc.* Obtenido de https://www.dwavesys.com/sites/default/files/D-Wave%202000Q%20Tech%20Collateral_0718web.pdf

Google. (2024). *Google Quantum AI. Construcción de sistemas cuánticos escalables.* Obtenido de https://quantumai.google/research

King, A., Raymond, J., Lanting, T., Isakov, S., & Mohseni, M. (18 de febreo de 2021). *Nature Comunication. Scaling advantage over path-integral Monte Carlo in quantumsimulation of geometrically frustrated magnets.* Obtenido de https://www.nature.com/articles/s41467-021-20901-5

Law, M. (07 de noviembre de 2023). *Technology Magazine. Top 10: Quantum computing companies.* Obtenido de https://technologymagazine.com/articles/top-10-quantum-computing-companies

McGeoch, C. (2014). *Springer Link. Adiabatic Quantum Computation and Quantum Annealing.* Obtenido de https://link.springer.com/book/10.1007/978-3-031-02518-1

Milenio. (06 de 12 de 2023). *UNAM, la primera institución académica en America Latina con computadoras cuánticas.* Obtenido de https://www.milenio.com/tecnologia/unam-adquiere-computadoras-cuanticas-es-la-primera-institucion-en-al

Millán, V. (2023). *ThinkBig Quantum Computing. Radiografía de la computación cuántica en 2024: qué empresas están empujando el próximo gran salto tecnológico.* Obtenido de https://blogthinkbig.com/radiografia-computacion-cuantica

Modern Physics. (2024). *Modern Physics. Uniones Josephson : Tecnología Cuántica, Aplicaciones y Avances.* Obtenido de https://modern-physics.org/uniones-josephson-tecnologia-cuantica-aplicaciones-y-avances/

Nowak, S. (18 de septiembre de 2024). *Nuclio. Computación cuántica: cómo funciona y qué son los ordenadores cuánticos.* Obtenido de https://nuclio.school/blog/computacion-cuantica-como-funciona-y-que-son-los-ordenadores-cuanticos/

Parra, F. (04 de diciembre de 2023). *Gaceta UNAM. Adquiere la Facultad de Ingeniería dos computadoras cuánticas.* Obtenido de https://www.gaceta.unam.mx/adquiere-la-facultad-de-ingenieria-dos-computadoras-cuanticas/

Ronnow, T., Wang, Z., & Troyer, M. (19 de junio de 2014). *Science. Defining and detecting quantum speedup.* doi:10.1126/science.1252319

Scarani, V., & Kurtsiefer, C. (17 de septiembre de 2014). *Inspire. The black paper of quantum cryptography: real implementation problems.* doi:10.1016/j.tcs.2014.09.015

Schneider, J., & Smalley, I. (05 de agosto de 2024). *IBM. What is quantum computing?* Obtenido de https://www.ibm.com/topics/quantum-computing

Stankevich, K., & Studenikin, A. (26 de noviembre de 2019). *Fisical Review. Neutrino quantum decoherence engendered by neutrino radiative decay.* doi:10.1103/PhysRevD.101.056004

Susskind, L. (27 de octubre de 2018). *Three Lectures on Complexity and Black Holes.* Obtenido de https://arxiv.org/pdf/1810.11563

TSTC en Vivo. (2024). *Explicación de la computación cuántica.* Obtenido de https://www.tstc.nl/nieuws/157

Yin, J., Li, Y.-H., & Liao, S.-K. (2020). *Nature. Entanglement-based secure quantum cryptography over 1,120 kilometres.* doi:10.1038/s41586-020-2401-y