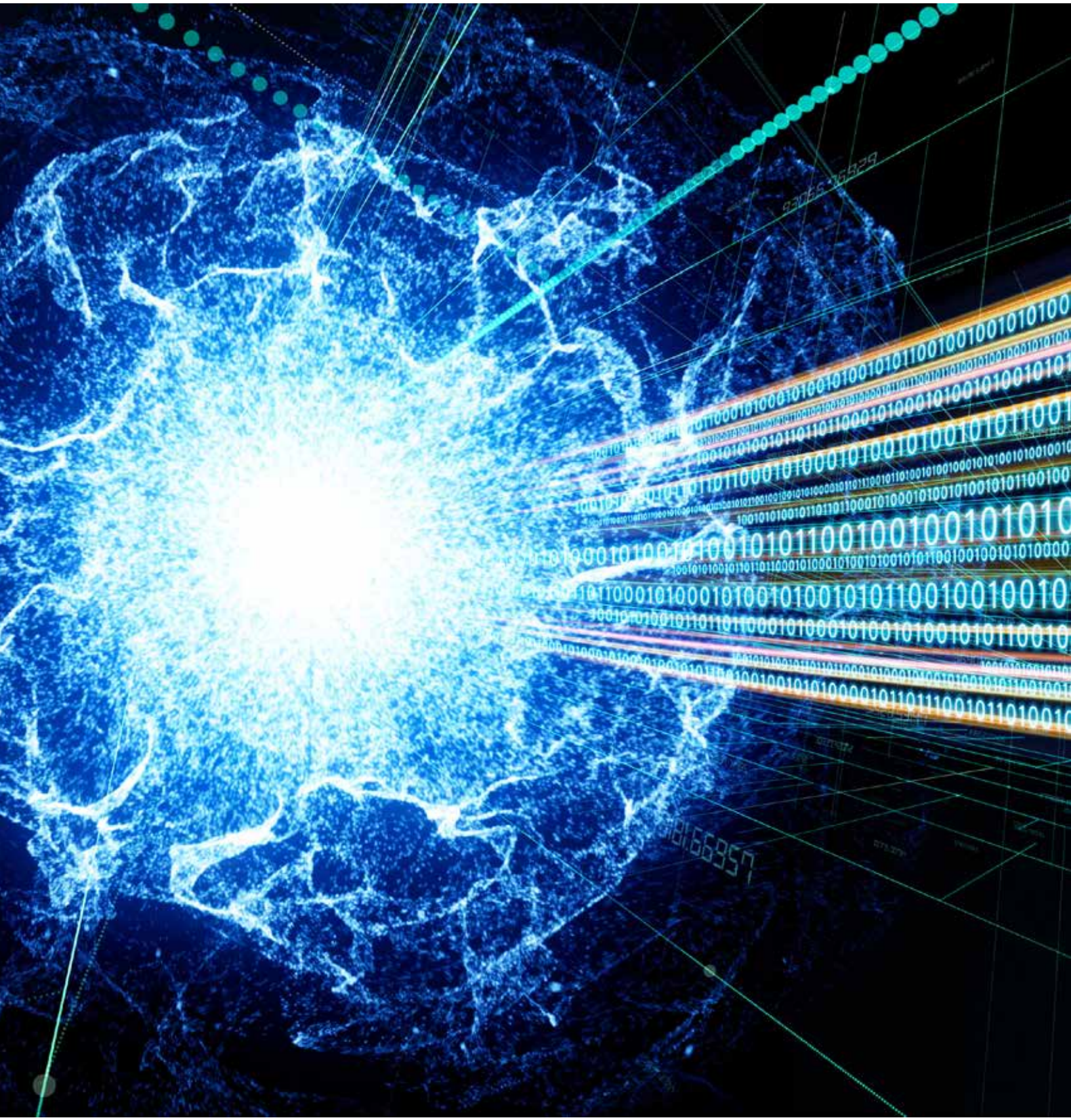


Licencia Internacional Creative Commons
Reconocimiento - No Comercial - Compartir Igual 4.0

ISSN 2215-5910
Investigación

¿ES LA COMPUTACIÓN CUÁNTICA EL FIN DE LA COMPUTACIÓN CLÁSICA?

Jorge Zapata Godoy
Emilio Brenes Pacheco
César Rodríguez Bravo

RESUMEN

La investigación se realiza con el objetivo de relacionar la computación clásica y la computación cuántica, así como determinar cuáles serán las implicaciones que podríamos ver en un futuro. Como consecuencia, surgen las preguntas: ¿Será la computación clásica eventualmente reemplazada por su contraparte cuántica? ¿Vendrá esta tecnología a revolucionar totalmente el viejo paradigma de las computadoras clásicas o tendrá una aplicación específica en ciertas industrias y se complementará con las computadoras actuales? En este artículo responderemos a ambas preguntas por medio de la ejecución de varios algoritmos de prueba cuyos resultados son la base de nuestro análisis. Cabe destacar que este artículo no se basa en simulaciones, sino en ejecuciones reales de algoritmos cuánticos en una computadora cuántica de 15-qubits.

Palabras claves: computación cuántica, algoritmo de Shor, criptografía, Qiskit, qubits.

ABSTRACT

The research is carried out with the aim of relating classical computing and quantum computing and thus determining what will be the implications that we could see in the future. As a consequence of the above, the questions arise: Will classical computing eventually be replaced by its quantum counterpart? Will this technology completely revolutionize the old paradigm of classical computers or will it have a specific application in certain industries and will it be complemented with current computers? In this article we will answer both questions by running various test algorithms whose results are the basis of our analysis. Notably, this article is not based on simulations but on actual runs of quantum algorithms on a 15-qubit quantum computer.

Key words: quantum computing, Shor's algorithm, cryptography, Qiskit, qubits.

Jorge Zapata es Investigador de Inteligencia Artificial en Ainnova Tech, Desarrollador y Director de Tecnologías en Neural Coders, Especialista en Cyberseguridad y estudiante de Ingeniería en Ciencia de Datos en LEAD University; Emilio Brenes es estudiante de Ingeniería en Ciencia de Datos en LEAD University y César Rodríguez es Profesor de Lead University, Máster en Cyberseguridad e Inventor con más de 100 aplicaciones a patentes en Estados Unidos, Europa y China.

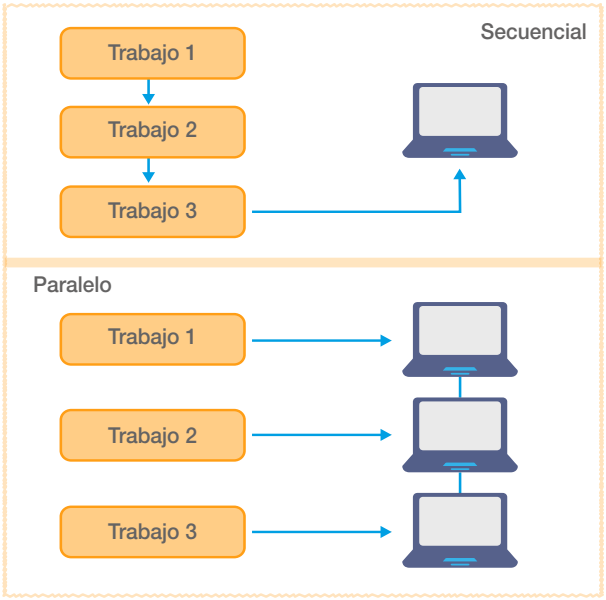
INTRODUCCIÓN

Como bien lo menciona la ley de Moore, la capacidad computacional se ha duplicado cada 2 años desde la creación del primer ordenador [1]. Sin embargo, la principal limitación de las computadoras clásicas (las computadoras que utilizamos actualmente) es que tienen que resolver cada tarea en secuencia y por lo tanto conforme el tamaño del problema va aumentando, también el tiempo para encontrar su solución crece.

Frente a este dilema, los científicos e ingenieros han desarrollado toda una rama de informática denominada computación paralela que utiliza el poder colectivo de varias computadoras interconectadas (supercomputadoras) y que en sincronía se reparten el trabajo de procesamiento para aliviar los trabajos individuales como se muestra en la figura 1.

Sin embargo, seguimos arrastrando el límite impuesto por el paradigma binario (de 1 y 0) de los ordenadores actuales donde básicamente sólo tenemos dos estados para representar información y esto hace que el tiempo de ejecución de algunos trabajos (por ejemplo, en el campo de simulaciones científicas o encriptación) sea extremadamente largo (aquí hablamos de años o incluso décadas) a pesar de utilizar el equipo más potente de la actualidad.

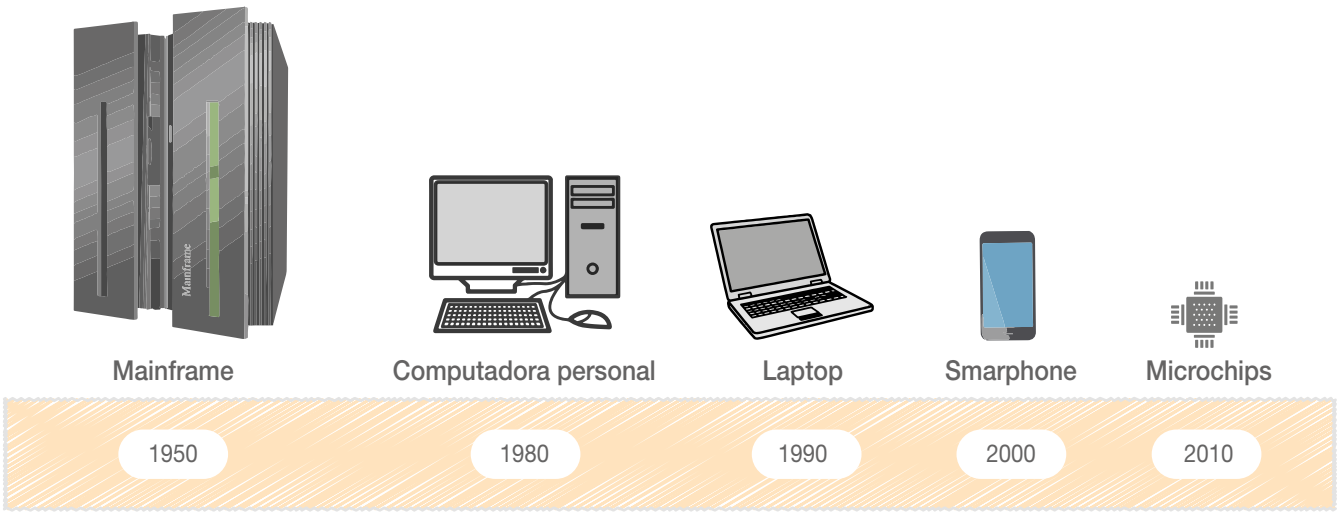
FIGURA 1. COMPUTACIÓN PARALELA, PARA DISTRIBUIR LA CARGA DE TRABAJO EN VARIAS COMPUTADORAS AL MISMO TIEMPO



Fuente: Elaboración propia.

Es aquí donde entra la computación cuántica, la cual sobrepasa significativamente las capacidades de las computadoras actuales (clásicas) que, a diferencia de estas, generan la información a partir de 1s y 0s,

FIGURA 2. LA LEY DE MOORE NOS INDICA, QUE CADA 2 AÑOS, SE DUPLICA LA CANTIDAD DE TRANSISTORES EN UN MICROPROCESADOR, LO QUE PERMITE CONSTRUIR MÁQUINAS CADA VEZ MÁS PEQUEÑAS Y POTENTES (CON MEJORES CAPACIDADES DE PROCESAMIENTO)



Fuente: Elaboración propia.

pero de forma paralela, es decir, tanto el 1 como el 0, se puede ejecutar en la misma computadora y segmento de tiempo. Esto hace que el tiempo de ejecución de algunas tareas de procesamiento complejo sea realmente muchísimo menor.

En las últimas dos décadas, con el desarrollo por parte de grandes compañías como IBM y Google, surgen proyectos muy interesantes producto del extenso desarrollo e investigación realizados en computación cuántica. Estos sistemas son conocidos como IBM-Q y Sycamore respectivamente, y permiten la ejecución de programas que potencien las maravillas del paradigma cuántico el cual abre nuevas posibilidades de lo que previamente se consideraba inviable.

Como consecuencia a lo mencionado previamente, surge la pregunta: *¿Será la computación clásica eventualmente reemplazada por su contraparte cuántica?*

¿Vendrán estas computadoras a revolucionar totalmente el viejo paradigma de las computadoras clásicas o tendrán una aplicación específica en las industrias y se complementarán con las actuales? Para esto, se realizó una demostración que expone las debilidades y fortalezas de ambas por medio de análisis criptográficos como base del estudio.

Para desarrollar nuestro objetivo, nos basaremos en la comparación del tiempo de ejecución del mismo algoritmo de desencriptación en una computadora cuántica real versus en una computadora clásica. El tiempo de ejecución de un algoritmo es un indicador del tiempo que le toma a una computadora completar todas las operaciones de un algoritmo y expresa su comportamiento en función al tamaño del problema. Con base en este dato, se puede determinar la diferencia (delta) en el tiempo requerido por ambas en quebrantar el cifrado de un mensaje.

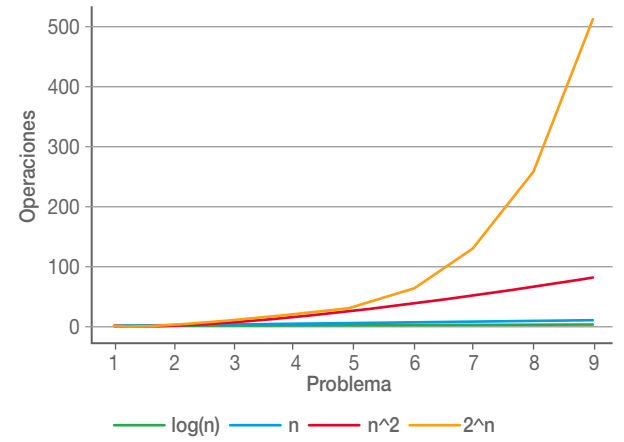
COMPUTADORAS CLÁSICAS VERSUS CUÁNTICAS

El campo de las tecnologías digitales se ha caracterizado por realizar cientos de operaciones en muy poco tiempo, las únicas limitaciones que presenta son por la naturaleza de la física [2]. Las **computadoras clásicas**, las utilizamos todos los días, desde un teléfono celular hasta una computadora de escritorio, todas forman parte de nuestras vidas.

Tomando en cuenta las capacidades actuales de las computadoras clásicas en diferentes aplicaciones de estudio, estas presentan ciertas limitaciones pero, ¿qué pasaría si pudiéramos incrementar las capacidades de la computación clásica?

Los últimos avances de la ciencia nos han demostrado que esto sí es posible por medio de las computadoras cuánticas, las cuales durante muchos años no se tuvo claro si realmente tendrían más poder computacional que las computadoras clásicas. Sin embargo, esto se demostró radicalmente en 1994 con el trabajo de Peter Shor [2].

FIGURA 3. DIFERENTES TIEMPOS DE EJECUCIÓN DE UN PROBLEMA, HACIENDO REFERENCIA AL TRABAJO DE SHOR



Fuente: Elaboración propia.

Peter Shor, un matemático e investigador del MIT (Instituto Tecnológico de Massachusetts) que ha sido referente en investigaciones relacionadas con la computación cuántica, comprobó que las computadoras cuánticas pueden procesar la información mucho más rápido que una computadora clásica, como se observa en la figura 3, Shor se encargó de comprobar que una computadora cuántica puede resolver problemas relacionados con la criptografía actual en un tiempo n^2, como se observa en la línea color magenta de la figura, la línea naranja eleva los tiempos para resolver un problema de forma exponencial y las últimas líneas azules, tienen un tiempo de resolución de un problema de forma lineal, este último tiempo es realmente difícil de lograr para problemas de criptografía.

A partir de estos conceptos, y gracias a las investigaciones realizadas sobre la computación cuántica, los resultados han sido sorprendentes a nivel de procesamiento, pero entonces, ¿qué es una máquina cuántica?

Para explicar esto de una manera sencilla, necesitamos comprender estos tres conceptos que la hacen diferente de la computación clásica: **teletransportación, entrelazamiento y superposición.**

Empecemos con este ejemplo. Hace mucho tiempo los medios de comunicación anunciaron que un equipo de la Universidad Nacional Australiana había logrado *"teletransportar"* un rayo láser. El rayo desapareció de un lugar (y en un abrir y cerrar de ojos), reapareció desplazado un metro de distancia desde el punto de origen en el espacio. Este concepto de desaparecer de un lugar y aparecer en otro, es el que conocemos en las películas como teletransportación [3].

La teletransportación es el concepto base de la computación cuántica. Este se refiere a transportar la información desde una localización hacia otra.

Las unidades básicas de información que se teletransportan en una computadora cuántica se conocen como **qubits.** A diferencia de los **'bits'** (que son la unidad de procesamiento para las computadoras clásicas), los **qubits** pueden tomar varios estados simultáneamente en 0 y 1 al mismo tiempo, y con esta propiedad pueden desarrollar cálculos que no puede hacer un ordenador convencional. Esta es la principal razón por la cual la computadora cuántica es más rápida que una computadora clásica, con cada **qubit** que se añade al procesamiento los estados cuánticos pueden tomar 2^n valores, a esto se le conoce como **superposición**.

Por último, la propiedad cuántica conocida como **entrelazamiento** hace referencia a que el estado cuántico (el valor de cada qubit) de todos los **qubits** en el sistema no se puede describir de forma independiente a los demás, incluso cuando están separados por una gran distancia. En otras palabras, cada **qubit** va a afectar el estado de todos los demás **qubits**. Esta propiedad no tiene un equivalente en el mundo clásico y es uno de los grandes diferenciadores entre la computación cuántica y la computación clásica.

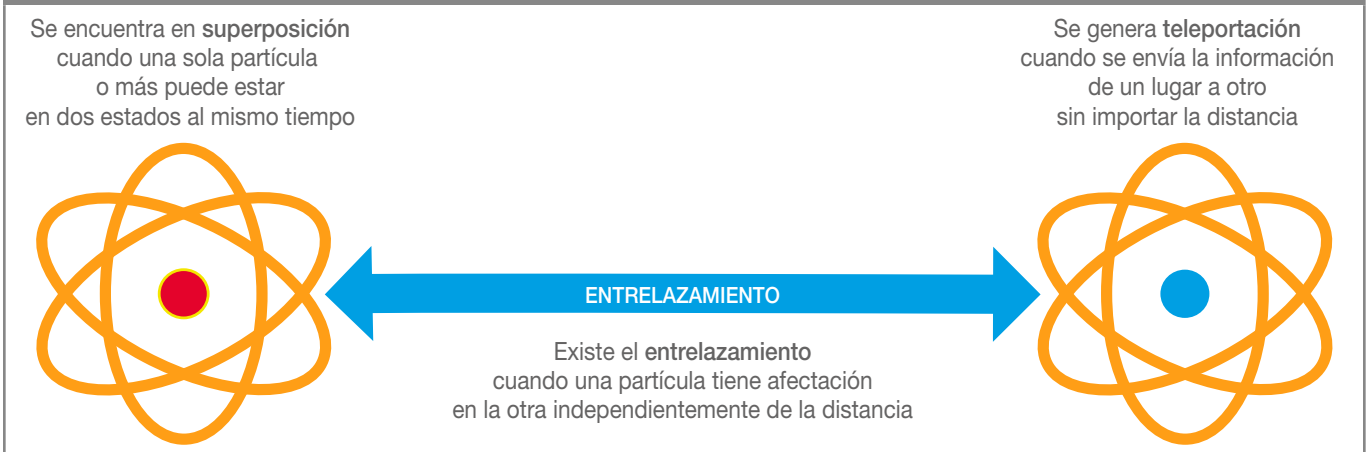
No obstante, se debe tomar en cuenta que, al día de hoy, las computadoras cuánticas son sistemas muy primitivos asimilables a una calculadora de principios del siglo pasado pero su capacidad de cálculo para determinados problemas es mucho más alta que un ordenador convencional.

METODOLOGÍA

El objetivo de la investigación fue comparar el desempeño del método clásico contra su contraparte cuántica en la resolución de un mismo problema. Como punto de referencia se tomó el tiempo que tarda en desencriptar un algoritmo de curvas elípticas.

Este es utilizado con regularidad para cifrar el intercambio de información en las redes, asegurar la integridad de las comunicaciones digitales y protegerlas de cualquier atacante o adversario que intente acceder a su contenido indebidamente. Para verlo en un ejemplo más claro, este algoritmo es el que se usa para asegurar las conversaciones que hacemos todos los días por WhatsApp.

FIGURA 4. LA SUPERPOSICIÓN DE ESTADOS, ES UNA CARACTERÍSTICA QUE NO ESTÁ PRESENTE EN LA COMPUTACIÓN CLÁSICA



Fuente: Elaboración propia.

Para lograr esto, fue necesario desarrollar un código para computadoras cuánticas y otro código para computadoras clásicas y que ambos fueran capaces de romper el algoritmo de las curvas elípticas, así como registrar el tiempo que ambas tomaron en hacerlo.

Para el algoritmo cuántico se utilizó la implementación del ***algoritmo de Shor***, el cual acelera el problema de la factorización de números primos.

En el caso de la computación clásica, se usó el algoritmo de ***Baby Step Giant Step*** desarrollado por Daniel Shank, el cual es un procedimiento diseñado para encontrar el exponente que cumple la igualdad para un campo finito de logaritmos discretos (que es la base fundamental de algoritmos de encriptación actuales por medio de curvas elípticas).

$$h = g^x \pmod{p}$$

Este problema consiste en encontrar el logaritmo discreto de h dado p como un número primo y la base g para establecer la igualdad encontrando el exponente de g.

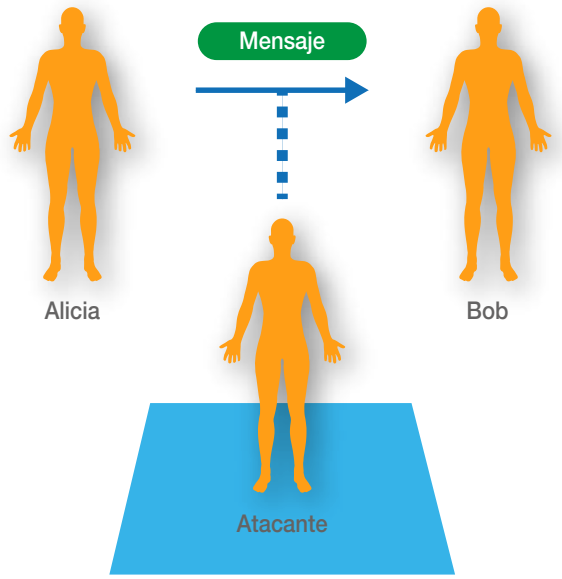
La seguridad de la criptografía actual, depende en gran medida del supuesto que la factorización de grandes números primos es una tarea lo suficientemente compleja para que el tiempo necesario de llevarla a cabo sea tan alto que una vez que el atacante logre hacerlo, la información interceptada ya no tiene valor para ser utilizada.

El dilema se encuentra que al cumplir esta igualdad tendremos la posibilidad de encontrar la clave privada de encriptación de un mensaje y esto implica que la privacidad de las comunicaciones se puede ver vulnerada. (figura 5).

Para la implementación del código del algoritmo **Baby-Step, Giant-Step**, utilizamos la plataforma digital de **Qiskit**, el cual es una herramienta desarrollada por la comunidad de software libre que permite la creación y manipulación de programas cuánticos y correrlos en prototipos de máquinas cuánticas de IBM Quantum Experience. Básicamente **Qiskit** es un lenguaje de alto nivel para la interacción entre un humano y la interfaz de una computadora cuántica que abstrae la dificultad de este proceso.

Otra base importante, fue el **algoritmo de Shor**, el cual es un algoritmo probabilístico, que permite a una computadora cuántica encontrar un factor no trivial de un gran número compuesto N en un tiempo acotado en un polinomio en Log_N.

FIGURA 5. EL MENSAJE PUEDE SER DESENCRIPTADO POR EL ATACANTE QUE LO INTERCEPTA Y ASÍ PUEDE LEER EL CONTENIDO DEL MENSAJE



Fuente: Elaboración propia.

Como se cree ampliamente que no existe un algoritmo de factorización de tiempo polinomial para una computadora clásica, el resultado de Shor indica que una computadora cuántica puede realizar eficientemente cálculos interesantes que son intratables en una computadora clásica [3].

Esto volvió posible ejecutar en una computadora cuántica real, resolver el problema de logaritmos discretos con la misma factorización y ecuación implementada para computadoras clásicas.

Como mencionamos, **Qiskit** fue seleccionada como la herramienta principal ya que para el desarrollo de la investigación era fundamental poder ejecutar código en una computadora cuántica y **Qiskit** provee la interfaz más actualizada y conveniente para hacerlo.

Cabe notar que la cantidad de qubits disponibles tiene un efecto en los resultados de ejecución del programa por lo que dada la tecnología disponible solo fue posible utilizar una computadora con 15 qubits. Sin embargo, para problemas pequeños como este, la cantidad de qubits no es un factor influyente.

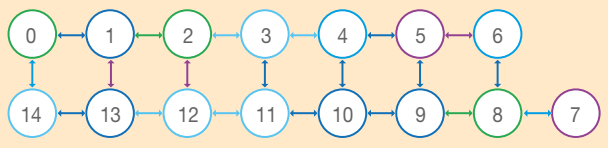
El problema que vamos a resolver se basa en una fórmula compleja de números primos. En ella también están sentadas las bases de la criptografía actual y vamos a utilizar el trabajo de Peter Shor y la creación de

Daniel Shank para comprobar los tiempos de ejecución del mismo problema en una computadora cuántica y una computadora clásica.

Las pruebas se realizaron utilizando la factorización de un número primo N como el módulo de la ecuación $h = g^x \pmod{p}$ en p, y este número era representado por 15 para la computadora cuántica y la computadora clásica a través de la instancia para desarrollo de modelos de IBM-Q.

Tomando en cuenta el concepto de los estados en superposición de una computadora cuántica (cuando sus estados se encuentran en 2^n, siendo n la cantidad de qubits), al utilizar menos qubits, la superposición es menor, por lo tanto, se pierde esta propiedad de procesamiento que permitiría ser más potente que las computadoras clásicas. Una representación de los qubits, se encuentran en la figura 6.

FIGURA 6. QUBITS REPRESENTADOS EN UN DIAGRAMA DE UNA COMPUTADORA CUÁNTICA REAL Y COMO ESTÁN INTERCONECTADOS PARA GENERAR LA SUPERPOSICIÓN



Fuente: Qubits de una instancia de IBMQ.

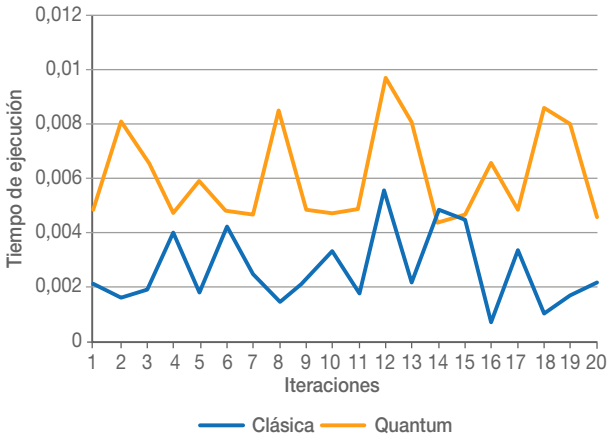
RESULTADOS Y DISCUSIÓN

Increíblemente los resultados en tiempos de ejecución para resolver el problema planteado, indican que la computadora clásica tuvo una media de **0,0026** milisegundos en tiempo de ejecución equivalente a una diferencia del **60% más rápido que una computadora cuántica**. Esto difiere del resultado esperado el cual suponía que correr el código utilizando las capacidades del mundo cuántico iba a acelerar notablemente el tiempo para resolver el cifrado.

¿Esto quiere decir entonces que las computadoras clásicas van a tener un mejor desempeño en ciertos casos específicos?

Como se observa en la figura 7, los resultados de ejecución en una computadora cuántica que cuenta con 15 qubits (IBM-Q), mostraron un tiempo promedio de **0,006** milisegundos, esto equivale a una diferencia relativa **2,29 veces más lenta** que la computadora clásica.

FIGURA 7. RESULTADOS DE EJECUCIÓN DEL ALGORITMO BABY STEP, GIANT STEP EN UNA COMPUTADORA CLÁSICA Y EL ALGORITMO DE SHOR EN UNA COMPUTADORA CUÁNTICA PARA RESOLVER EL PROBLEMA DE LOGARITMOS DISCRETOS, EN ESTE SE BASA LA ENCRIPTACIÓN ACTUAL DE CURVAS ELÍPTICAS



Fuente: Elaboración propia con los datos de la ejecución de los algoritmos en computadoras clásicas y computadoras cuánticas.

No todos los problemas computacionales serán resueltos más rápidamente por las computadoras cuánticas.

A pesar de que la **computación cuántica** se ha exhibido como el futuro de las tecnologías en ciencias computacionales, hemos demostrado que **no todos los problemas computacionales serán resueltos más rápidamente por las computadoras cuánticas**.

Esto se debe a que lidiar con las complejidades cuánticas como la superposición, entrelazamiento y teletransportación tiene un costo computacional que solo se logra compensar por los beneficios asociados a partir de cierto punto y ese punto es determinado por el tamaño del problema que se pretenda resolver y a este punto le llamamos: ***Punto de inflexión cuántico***.

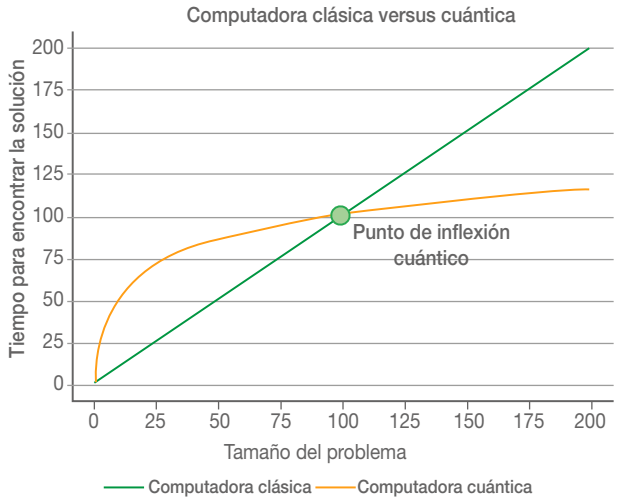
Por lo tanto, podemos definir que si el problema a resolver no es lo suficientemente grande (a nivel de procesamiento) entonces los costos adicionales que conlleva la ejecución cuántica no serán justificados dado que estos se logran maximizar en problemas de computación compleja.

En este caso, utilizar una computadora clásica resulta más conveniente ya que se trata de un problema fácil de resolver (pequeño) y por lo tanto se demostró que no es necesario recurrir a los súper poderes cuánticos (ya que en este caso específico es más lento y costoso).

Antes de pensar en adaptar tecnologías cuánticas, debemos analizar el ***punto de inflexión cuántico*** *para determinar si realizar ese trabajo en una máquina cuántica es eficiente y rentable.*

Por el contrario, si lo que se requiere es resolver un problema sumamente complejo o computacionalmente pesado, los beneficios brindados superarán los costos asociados y la computadora cuántica será una mejor opción al reducir significativamente el tiempo para encontrar una solución al problema.

FIGURA 8. TIEMPO PARA ENCONTRAR LA SOLUCIÓN DE UN PROBLEMA EN FUNCIÓN A SU TAMAÑO EN COMPUTADORAS CLÁSICAS Y CUÁNTICAS



Fuente: Elaboración propia.

La figura 8 ilustra el concepto de ***Punto de Inflexión Cuántico*** con dos curvas, cada una representando el tiempo en encontrar una solución para un problema.

La curva verde es el tiempo de ejecución de un algoritmo de búsqueda clásico y la curva naranja el de un algoritmo de búsqueda cuántico. En el eje X, tenemos el tamaño del problema y en el eje Y el tiempo de solución.

En la figura anterior, para un problema con un tamaño menor a 100 el algoritmo cuántico va a tener un peor desempeño que su contraparte clásica. Esto se observa con la curva naranja estando por encima de la verde lo que indica un mayor tiempo requerido.

A partir de cualquier problema mayor a 100 la relación se invierte y el algoritmo cuántico tomará menos tiempo que el clásico.

Dicho de otra forma, es a partir del ***Punto de Inflexión Cuántico*** que los beneficios superan a los costos y la computadora cuántica se vuelve la opción más favorable. El tamaño N del problema asociado al ***Punto de Inflexión Cuántico*** va a depender de la naturaleza y complejidad de la tarea a resolver.

También demostramos que ***no es rentable resolver todos los problemas utilizando una máquina cuántica***, esto es importante porque actualmente la creencia es que la computadora cuántica es mucho más rápida que la computadora clásica pero hemos demostrado que los problemas pequeños tienen un menor rendimiento en computadoras cuánticas.

¿Qué implicaciones prácticas tienen los resultados encontrados?

A diferencia de algunos mitos sobre la computación cuántica, se confirmó que esta no viene a reemplazar el rol de las computadoras clásicas, por el contrario, estas serán un complemento de las computadoras clásicas.

Lo que sí logrará la computación cuántica es expandir la curiosidad y el poder de la ciencia al permitir el abordaje y análisis de nuevos problemas sumamente complejos que previamente no se tenían las herramientas adecuadas para solucionar.

Con los resultados demostrados, las posibles aplicaciones en las industrias de la inteligencia artificial y el big data, son enormes ya que nos podría ayudar también a descubrir información y patrones que tengan un valor agregado para las empresas.

Recordemos que para procesar y realizar inteligencia artificial se requiere una gran cantidad de datos para que la computadora pueda aprender a partir de las tendencias encontradas, sin embargo, estos algoritmos están actualmente limitados a las computadoras clásicas. Es aquí donde la computación cuántica podría ayudar a mejorar la eficiencia de los modelos de inteligencia artificial.

Para dar un ejemplo, la computadora cuántica de Google, Sycamore, resolvió un problema en 200 segundos que a un supercomputador actual (el más rápido con el que se cuenta actualmente) tardaría 10.000 años en resolverlo.

Utilizar el término, ***Punto de Inflexión Cuántico***, es valioso para interiorizar el concepto y que este se considere en la toma de decisiones de las empresas que estén valorando la tecnología cuántica. Entender cuáles

tecnologías son las adecuadas previo al comienzo de un proyecto y elegir estas bajo un criterio científico y cuantificable puede ser la diferencia entre el fracaso y éxito del mismo.

Poder etiquetar un concepto tan complejo y referirse a este con un solo término, será de mucha utilidad para todas las conversaciones futuras que giren alrededor del contraste entre el paradigma cuántico y el clásico.

De igual forma, dado que los avances en tecnología cuántica están constantemente excediendo nuestras expectativas y empoderando cada vez más este paradigma, tener un punto de referencia para cuantificar el aporte del avance va a resultar indispensable. El ***Punto de Inflexión Cuántico*** es un candidato ideal para llenar este vacío por su habilidad para expresar la relación entre lo clásico y lo cuántico y cómo esta relación se ve afectada con cada gran hallazgo científico logrado.

CONCLUSIONES

De una forma impresionante (y casi inesperada), podemos afirmar que las tecnologías cuánticas ***no vendrán a sustituir*** la tecnología tradicional de las computadoras clásicas, al contrario, a partir de los resultados de esta investigación, se confirma que esta será un complemento ideal a la computación clásica en la resolución de problemas en los cuales estas no son tan eficientes.

Problemas complejos que requieren extensos cálculos matemáticos y grandes capacidades computacionales son el caso ideal para medir las características de las computadoras cuánticas y superar considerablemente el rendimiento y tiempo de ejecución de sus antecesores clásicos.

Para tareas simples que no presentan un reto computacional, como lo son la gran parte de las necesidades para las personas, las computadoras clásicas, al estar libres de la complejidad del paradigma cuántico, son una mejor opción más práctica, rentable y accesible.

Consecuentemente, surge la necesidad de identificar el punto a partir del cual las computadoras cuánticas se vuelven una opción más adecuada que las clásicas. Este punto dependerá de la naturaleza del problema a resolver y determina cuando, en términos del tamaño del problema, es más pertinente trasladarse de paradigma. Nosotros le llamamos: ***Punto de Inflexión Cuántico.***

Tener el conocimiento de la ubicación de este punto, va a resultar valioso para empresas que estén evaluando qué tecnologías incorporar a sus servicios, productos y proyectos. Esto porque el ***Punto de Inflexión Cuántico*** les permite discernir si el caso de negocio que están considerando se ve beneficiado por la aplicación de computadoras cuánticas.

Asimismo, facilita las conversaciones que pretenden comparar ambos paradigmas al abstraer la dificultad del concepto y proveer una forma fácil de comunicarlo.

Por último, este también es un punto de referencia muy práctico que permite analizar el impacto de nuevos descubrimientos científicos en el rendimiento y capacidad de las computadoras cuánticas en relación con las clásicas.

No obstante, sabemos que algunos de los inconvenientes actuales para el procesamiento a través de qubits están relacionados con la cantidad de los qubits que nos ofrecen las máquinas cuánticas actuales, por lo tanto, hasta próximas investigaciones donde tengamos más qubits disponibles, tendremos la posibilidad de resolver problemas aún más complejos y superar en gran medida las capacidades de las tecnologías digitales actuales.

BIBLIOGRAFÍA

[1] Brookshear, G. J. (2012). *Introducción a la Computación*. España: Pearson.

[2] Miquel, C. (2002). *Computadoras cuánticas*. Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires.

[3] Terán Pérez, D. M. (2012). *Introducción a la Computación Cuántica para Ingenieros.* México: Alfa-omega.

[4] Devabhaktuni, S.; Preskill, J.; Beckman, D. y Amalavoyal, N. C. (1996). Efficient networks for quantum factoring. *American Physical Society*, 54(2):1034-1063.