ANÁLISIS DE FORTALEZAS Y DEBILIDADES:

Si bien la computación cuántica ha avanzado dramáticamente durante la última década, sus aplicaciones potenciales aún no se han demostrado a gran escala. Es probable que tales demostraciones requieran avances en física, informática e ingeniería, ya que, las computadoras cuánticas son propensas a errores debido a la coherencia cuántica y las condiciones ambientales.[Grover's Algorithm]

Por otro lado, se dice que en el futuro, una computadora cuántica (QC) puede resolver algunos problemas mucho más rápido que una computadora clásica (CC), lo que se denomina ventaja cuántica, esto se debe a que la potencia de cómputo de QC está creciendo más rápido que la de CC. Una de las medidas del rendimiento de la Computadora Cuántica introducida por IBM es el Volumen Cuántico. Para lograr una ventaja cuántica en la próxima década, IBM declaró que “necesitan al menos duplicar el volumen cuántico de nuestros sistemas de computación cuántica cada año.” En enero de 2020, Chow y Gambetta confirmaron que IBM está en camino de alcanzar este objetivo con una nueva computadora cuántica de 28 qubits que demuestra el volumen cuántico de 32 [Quantum Advantage and Y2K].

Asimétrico:

Todos los algoritmos asimétricos actuales (RSA, ECC, DH, DSA) se pueden descifrar mediante computadoras cuánticas. Se basan en el problema de factorización prima o el problema del logaritmo discreto, que son fáciles de resolver en computadoras cuánticas utilizando el algoritmo de Shor.Matemáticos y criptógrafos utilizaron estos problemas de teoría de números para fundamentar la seguridad de los algoritmos asimétricos. Ahora tienen que buscar nuevos problemas matemáticos que las computadoras cuánticas no puedan resolver fácilmente. [Post Quantum Cryptography Techniques]

Actualmente odos los algoritmos asimétricos se basan en problemas matemáticos para los que la gente ha buscado soluciones durante siglos. Sin embargo, la debilidad que tienen es que las computadoras cuánticas son buenas en tareas paralelas que requieren un resultado al final. Dado que los algoritmos requieren solo un resultado al final, se puede usar una superposición de qubits para paralelizar todos los cálculos y luego se puede medir el resultado. Para evitar aprovechar el paralelismo de las computadoras cuánticas se pueden utilizar algoritmos que requieren varios resultados. De esta manera, el paralelismo de las computadoras cuánticas no se puede utilizar en toda su extensión.[Post Quantum Cryptography Techniques]

Simétrico:

Los algoritmos simétricos y las funciones hash son relativamente seguros en un mundo poscuántico. El algoritmo de Grover puede acelerar los ataques por complejidad de raíz cuadrada, sin embargo, la mayoría de los algoritmos se pueden volver a asegurar duplicando el tamaño de la clave. [Post Quantum Cryptography Techniques] Cuando se consideran aplicaciones del algoritmo de Grover, se debe enfatizar que la base de datos no se representa explícitamente. En cambio, se invoca un oráculo para evaluar un elemento por su índice. Leer una base de datos completa elemento por elemento y convertirlo en una

representación de este tipo puede llevar mucho más tiempo que la búsqueda de Grover. Para tener en cuenta tales efectos, el algoritmo de Grover se puede considerar como una solución a una ecuación o una restricción. En tales aplicaciones, el oráculo es una forma de verificar la restricción y no está relacionado con el algoritmo de búsqueda. Esta separación generalmente evita las optimizaciones algorítmicas, mientras que los algoritmos de búsqueda convencionales a menudo se basan en tales optimizaciones y evitan la búsqueda exhaustiva[Grover's Algorithm].

Algunas limitaciones importantes de la computadora cuántica de IBM[Grover's Algorithm].:

- problemas de coherencia:
  El dispositivo debe luchar constantemente contra el entorno que actúa para degradar la coherencia del sistema. Y, por lo tanto, la delicada información cuántica almacenada en una computadora cuántica es extremadamente susceptible al ruido. Los qubits deben mantenerse fríos o de lo contrario colapsarán fácilmente. El error debido al entrelazamiento de qubits es alto. Los errores de puerta multiqubit fueron mucho más altos que los errores de puerta de un solo qubit.

- La conectividad limitada entre los qubits: esta es otra de las limitaciones más importante, por lo tanto, existe la necesidad de emplear un gran número. de compuertas de intercambio que aumenta el conteo de compuertas (lo que se suma a los errores de compuerta) especialmente los cnots que tienen errores bastante altos y, por lo tanto, reducen en gran medida la fidelidad de estado esperada y también los circuitos se vuelven complejos y difíciles de comprender y depurar.

Los simuladores de IBM ya tienen una longitud de código limitada, por lo que se vuelve difícil implementar circuitos grandes o ampliar los circuitos para agregar puertas de corrección de errores o resolver el problema de la conectividad limitada agregando más intercambio. puertas. La implementación de la puerta tofolli para 16 qubits requirió muchos qubits adicionales o una gran cantidad de etapas, las cuales no son posibles en los dispositivos IBM actuales y, por lo tanto, implementar la búsqueda de Grover de 16 qubits en los simuladores de IBM y los dispositivos reales no era realista [Grover's Algorithm].