OBJETIVO:

los principales objetivos del survey es demostrar que teóricamente se puede romper sistemas criptográficos simétricos y asimétricos, así como también dar a conocer los principales algoritmos que se usan para lograrlo como el algoritmo de shor y el algoritmo de grover, además de tener en cuenta que para evitar ataques cuánticos se usan técnicas denominadas criptografía post cuántica.

Algoritmo grover:

Es posible utilizar el algoritmo de Grover para romper el cifrado AES (Advanced Encryption Standard), que es uno de los cifrados más utilizados en la actualidad. Dicho algoritmo puede buscar en una base de datos de posibles claves hasta encontrar la clave correcta en un número de pasos cuadrático en el tamaño de la base de datos, lo que significa que puede encontrar la clave correcta mucho más rápido que un algoritmo clásico. Pero, para utilizar el algoritmo de Grover de esta manera, se necesita una computadora cuántica a gran escala.

Algoritmo Shor:

El algoritmo de Shor es un algoritmo diseñado para factorizar números grandes en sus factores primos y esto es importante porque la factorización de números grandes es un problema difícil de resolver con la tecnología de computación clásica, pero Shor puede hacerlo de manera eficiente utilizando la mecánica cuántica y en un tiempo polinomial. Dicho algoritmo también tiene aplicaciones en la criptografía cuántica y en la simulación de sistemas cuánticos complejos, shor también resuelve el problema de los logaritmos discretos. Sin embargo también requiere de una computadora cuántica a gran escala.

Transformada cuántica de fourier:

La transformada de Fourier cuántica es una herramienta matemática utilizada en la computación cuántica para analizar funciones en el espacio de frecuencias. Dicho algoritmo se basa en la transformada de Fourier clásica, pero utiliza operaciones cuánticas en lugar de operaciones matemáticas clásicas, además La QFT tiene aplicaciones en la búsqueda cuántica como la factorización de números y la simulación de sistemas cuánticos, pero también requiere de una computadora cuántica a gran escala.

y digo a gran escala ya que con ello se conseguirá ser implementado de manera efectiva.

ahora para tener más claro, **¿Qué es el problema de la escalabilidad?**

Uno de los principales desafíos en la implementación de la computación cuántica a gran escala es la escalabilidad. Para poder realizar operaciones cuánticas complejas, se necesitan muchos qubits y una alta conectividad entre ellos. Sin embargo, construir una computadora cuántica a gran escala es un desafío técnico, ya que se requiere una alta precisión y control para manipular y conectar qubits de forma efectiva. Además, el ruido y la pérdida de coherencia en los qubits pueden aumentar a medida que se aumenta el número de qubits, lo que dificulta la realización de operaciones cuánticas precisas.

TAXONOMÍA:

En esta sección estoy clasificando en los dos tipos de criptografía clásica que existen, simetrica y asimetrica

En la criptografía simétrica tenemos al algoritmo grover y la transformada cuántica de fourier como principales algoritmos que vulneran dicho sistema criptográfico.

y en la criptografía asimétrica también se encuentra la transformada cuántica de fourier y el algoritmo shor como algoritmos principales para romper los algoritmos asimétricos

ANÁLISIS DE FORTALEZAS Y DEBILIDADES

Se dice que en el futuro, una computadora cuántica podría resolver algunos problemas mucho más rápido que una computadora clásica, lo que se denomina como ventaja cuántica

Sin embargo, aún no se ha podido explotar al máximo las ventajas de una computadora cuántica debido a que aún no se tiene lo suficiente y además de los problemas de coherencia y errores ambientales.

- **Ataque a la criptografía asimétrica:**

  Todos los algoritmos asimétricos como el RSA pueden resolverse con una computadora cuántica, ya que se basan en la descomposición de números primos y logaritmos discretos. Por lo que se deberá buscar nuevos problemas matemáticos que las computadoras cuánticas no puedan resolver fácilmente

- **Ataque a la criptografía simétrica:**

  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.

- **Problemas de coherencia:**

  Uno de los principales desafíos en la implementación de la computación cuántica es mantener la coherencia de los qubits, que son las unidades básicas de información. La coherencia se refiere a la capacidad de un qubit para mantener un estado cuántico definido durante un tiempo prolongado. Sin embargo, el ruido y las interacciones con el entorno pueden causar la pérdida de coherencia en los qubits, lo que dificulta la realización de operaciones cuánticas precisas.

- **Conectividad limitada entre qbits:**

  Los qubits se deben conectar entre sí para poder realizar operaciones cuánticas complejas, pero esto puede ser difícil de lograr si la conectividad entre ellos es

limitada. Una forma de abordar este problema es utilizar qubits que puedan ser conectados de forma más eficiente, como qubits basados en iones atrapados o en átomos en una red cristalina. También se pueden utilizar técnicas de "teleportación cuántica" para conectar qubits que no están directamente conectados entre sí.

¿Qué es la teletransportación cuántica?

La teleportación cuántica es un fenómeno en el que se pueden transmitir las propiedades de un qubit a otro qubit a través de un canal de comunicación cuántica, sin necesidad de enviar el qubit físico mismo. Esta técnica se basa en las leyes de la mecánica cuántica y utiliza el entrelazamiento cuántico para transmitir la información. La teleportación cuántica se ha demostrado en experimentos con sistemas pequeños, pero todavía se encuentra en etapas tempranas de desarrollo. Se espera que en el futuro la teleportación cuántica pueda utilizarse para transmitir información de forma más segura y eficiente, así como para conectar qubits que no están directamente conectados entre sí en una computadora cuántica.

CRIPTOGRAFÍA POST CUÁNTICA:

La criptografía post-cuántica se refiere a las técnicas de cifrado que serían resistentes a los ataques utilizando computación cuántica. POR OTRO LADO, Actualmente, la mayoría de los sistemas de cifrado utilizados en la industria se basan en la dificultad de resolver ciertos problemas matemáticos, como la factorización de números grandes. Sin embargo, se ha demostrado que la computación cuántica puede resolver estos problemas de forma más eficiente que la computación clásica, lo que significa que los sistemas de cifrado actuales podrían ser vulnerables a ataques cuánticos en el futuro. eNTONCES La criptografía post-cuántica se enfoca en desarrollar nuevas técnicas de cifrado que sean resistentes a ataques cuánticos. Sin embargo, todavía se encuentra en etapas tempranas de desarrollo y conforme avance la tecnología cuántica se irá mejorando estas técnicas

CONCLUSIONES:

Sabemos que en la actualidad la computación cuántica está creciendo de manera muy rápida y es por ello que muchas empresa están invirtiendo en la seguridad post cuántica, así como también ya se conoce cuales son los algoritmos que amenazan la criptografía simetrica y asimetrica, ya que estos pueden resolverlos en tiempo polinomial, sin embargo los principales problemas presentes en la computación cuántica, como el entrelazamiento de qubits, el ruido, la coherencia, la escala, aun no nos permite que explotemos al máximo su potencial por lo que actualmente es imposible resolver los problemas de factorizacion de numeros grandes como los de 2048 bits.

en cuanto a trabajos futuros:

para mejorar este problema, me dispongo a investigar sobre las técnicas de compresión de datos, y así reducir la cantidad de información necesaria para representar un número grande, lo que permite trabajar con él, utilizando un número reducido de qubits

y el ruido es una interferencia externa que puede afectar el estado cuántico de un sistema y causar errores en los cálculos por tal motivo Para mejorar este problema, investigaré los diferentes enfoques como la corrección de errores y la utilización de técnicas de reducción de ruido en los circuitos cuánticos.

Los principales desafíos en la implementación de la computación cuántica son:

1. **La coherencia de los qubits**: mantener la coherencia de los qubits durante un tiempo prolongado es un desafío importante en la computación cuántica, ya que el ruido y las interacciones con el entorno pueden causar la pérdida de coherencia.
2. **La escala**: construir una computadora cuántica a gran escala es un desafío técnico, ya que se necesitan muchos qubits y una alta conectividad entre ellos para realizar operaciones cuánticas complejas.
3. **El ruido**: el ruido es una interferencia externa que puede afectar el estado cuántico de un sistema y causar errores en los cálculos. Reducir el impacto del ruido en la computación cuántica es un desafío importante.
4. **La programación cuántica**: desarrollar lenguajes de programación y herramientas adecuadas para programar computadoras cuánticas es un desafío importante para aprovechar plenamente el potencial de la computación cuántica.
5. **La integración con la tecnología clásica**: la computación cuántica y la computación clásica son dos tecnologías muy diferentes, por lo que integrarlas eficientemente es un desafío importante.