En la década de 1980 el reconocido físico teórico Richard Phillips Feynman notó que la simulación de ciertos efectos de la mecánica cuántica en una computadora clásica no es muy eficiente, debido a esto se ideó la construcción de computadoras cuánticas pero este conlleva un desarrollo lento debido a su complejidad. En 1994 el matemático del MIT Peter Shor Williston diseñó un algoritmo cuántico de tiempo polinomial para la factorización de números enteros[1].

En el mundo de la informática se conoce el bit, a su vez existe el bit cuántico o también llamado qbit, donde este puede ponerse en un estado de superposición que codifica al 0 y al 1. En la computación clásica se usan los procesos paralelos para disminuir el tiempo de procesamiento de algunos cálculos, por otro lado en un sistema cuántico se usa el paralelismo de forma masiva. A diferencia de la computación clásica en donde se puede leer el resultado de un thread paralelo, en la computación cuántica debido que la medición es probabilística no se puede elegir qué resultado leer por lo que el acceso a los resultados es totalmente restringido y para acceder se realiza una medición, dicha solución se viene mejorando con el pasar de los años en donde se involucra algoritmos conocidos como la factorización de Shor, el algoritmo de Grover, sin embargo todas las propuestas recientes tiene problemas escalabilidad y se requiere de un gran avance para sobrepasar las decenas de qbit [1].

Hoy en día muchos asumen que implementar un algoritmo criptográfico "irrompible" es imposible, por lo que en la actualidad se centran más en resistir el ataque. Los algoritmos de encriptación más usados son el RSA, DES, AES; si bien es cierto estos algoritmos están diseñados para resistir ataques de las computadoras actuales, pero es cuestión de tiempo para que estos sistemas sean cada vez menos resistentes. Este problema permitió el desarrollo de la criptografía cuántica en la que se basa en las leyes de la mecánica cuántica con el objetivo de proteger el secreto de los mensajes [2]. Actualmente con las constantes investigaciones acerca de la computación cuántica, estamos por entrar a una nueva era de la criptografía en la que se plantea un nuevo protocolo de distribución de

claves cuánticas BB84 desarrollado por Charles Bennet y Gilles Brassard en 1984 [3].

Los algoritmos cuánticos representan un peligro para la criptografía clásica; el más famoso y amenazante es el algoritmo de Shor ya que este resuelve el problema de factorización de enteros así como también el problema de logaritmos discretos en tiempo polinomial [4]. La transformada Cuántica de Fourier juega un papel importante y se encuentra en el núcleo de los algoritmos.

Actualmente hay 3 direcciones importantes de investigación de los ataques de clave pública de computación cuántica[5]:

1. Mejorar, modificar, simplificar el algoritmo de Shor y si fuera posible inventar uno que supere a Shor.
2. Algoritmos de ataque cuántico basados en computación cuántica adiabática
3. algoritmos de ataque cuántico basados en el principio de recorrido cuántico

Hoy en día el uso de la computación clásica en la vida cotidiana es normal y para el intercambio de información se hace uso de la criptografía de clave pública como el RSA (Rivest, Shamir y Adleman), en donde la encriptación de envío de datos desde un emisor hacia un receptor es confiable. La protección que brinda diversos algoritmos criptográficos clásicos hasta cierto punto son altamente seguros y eficientes, pero en algún momento estos dejaran de serlo y más aún con el desarrollo de la computación cuántica.

En este survey se muestran conceptos fundamentales de la computación cuántica, así como también se mostrarán algoritmos cuánticos y sus funcionalidades. Por otro lado la investigación en este survey se enfocará en vulnerar la seguridad del cifrado clásico de clave pública, haciendo uso de la idea del algoritmo de Shor para enfrentar la solución de logaritmos discretos y la factorización de números enteros de gran tamaño, así como

también la importante aplicación y el gran papel que juega la Transformada Cuántica de Fourier.

https://www.welivesecurity.com/la-es/2016/06/14/computacion-cuantica-armagedon-criptografico/

////// EXPOSICIÓN //////////////////
slide 1
¿Cómo nace la idea de computación cuántica?
En 1980 el físico Feynman notó que la simulación de ciertos efectos de la mecánica cuántica en una computadora clásica no es muy eficiente, es por ello que ideó las nociones de lo que quería lograr con una computadora cuántica, pero también notó que el desarrollo de una de estas sería muy lenta, pese a que aún se encontraba en una época en donde la computación clásica se encontraba en desarrollo.

slide 2:
¿Qué es Computación Cuántica?
Entonces, ¿qué es computación cuántica?
La computación cuántica es un paradigma de computación distinto al de la computación clásica... y esta se basa en el uso de qubits, que es una especial combinación de unos y ceros, en otras palabras el qubit puede ponerse en un estado de superposición que codifica al 0 y al 1.

slide 3:

Principales Algoritmos Cuánticos

- Grover Algorithm (Lov Grover en 1996): también conocido como algoritmo de búsqueda cuántica, y se basa en la búsqueda no estructurada que encuentra con alta probabilidad la entrada única a una función de caja negra que produce un valor de salida particular, usando solo O (sqrt(N) evaluaciones de la función, donde N es el tamaño del dominio de la función.

- Quantum Fourier Transform: es una transformación lineal en bits cuánticos y es el análogo cuántico de la transformada discreta de Fourier . La transformada cuántica de Fourier es parte de muchos algoritmos cuánticos , en particular el algoritmo de Shor para factorizar y calcular el logaritmo discreto , el algoritmo de estimación de fase cuántica para estimar los valores propios de un operador unitario y algoritmos para el problema del subgrupo oculto.

- Shor's algorithm(Peter Shor 1994): algoritmo de computadora cuántica para encontrar los factores primos de un número entero.

- Deutsch–Jozsa algorithm: es un algoritmo cuántico determinista que determina si una función está o no balanceada

slide 4:
¿Qué es criptografía?

- Confidencialidad. Es decir, garantiza que la información sea accesible únicamente a personal autorizado. Para conseguirlo utiliza códigos y técnicas de cifrado.
- Integridad. Es decir garantiza la corrección y completitud de la información. Para conseguirlo puede usar por ejemplo funciones hash criptográficas MDC, protocolos de compromiso de bit, o protocolos de notarización electrónica.
- Vinculación. Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado. Cuando se trata de una persona, se trata de asegurar su conformidad respecto a esta vinculación (content commitment) de forma que pueda entenderse que la vinculación gestionada incluye el entendimiento de sus implicaciones por la persona. Antiguamente se utilizaba el término "No repudio" que está abandonándose, ya que implica conceptos jurídicos que la tecnología por sí sola no puede resolver. En relación con dicho término se entendía que se proporcionaba protección frente a que alguna de las entidades implicadas en la comunicación, para que no pudiera negar haber participado en toda o parte de la comunicación. Para conseguirlo se puede usar por ejemplo firma digital. En algunos contextos lo que se intenta es justo lo contrario: Poder negar que se ha intervenido en la comunicación. Por ejemplo cuando se usa un servicio de mensajería instantánea y no queremos que se pueda demostrar esa comunicación. Para ello se usan técnicas como el cifrado negable.
- Autenticación. Es decir proporciona mecanismos que permiten verificar la identidad del comunicador. Para conseguirlo puede usar

por ejemplo función hash criptográfica MAC o protocolo de conocimiento cero.

y actualmente constantemente se estudia los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican

slide 5

Tipos de cifrado

Simétrica: Utiliza la misma clave para cifrar y descifrar el mensaje, que tienen que conocer, previamente, tanto el emisor como el receptor.

Asimétrica

- Clave pública: que se podrá difundir, sin ningún problema, a todas las personas que necesiten mandarte alguna información cifrada.
- Clave Privada: que no debe ser revelada nunca.

Aunque pueda parecer que la clave privada pudiese ser descubierta gracias a la pública en realidad no es así ya que se utilizan complejos algoritmos para generar las claves, que son muy resistentes a los ataques.

slide 6

Algoritmos de clave pública

- Ahora veamos Los sistemas de cifrado de clave pública más utilizados son
- RSA (para firma y encriptación),
- DSA (para firma)
- Diffie-Hellman (para acuerdo de clave).

un dato curioso pero importante es que en abril de 2016, investigadores de Canadá establecieron un nuevo récord en la factorización con computadoras cuánticas ya que se logró factorizar un número de 18 bits lo cual es demasiado pequeño para obtener la potencia de cálculo necesaria para factorizar un número entero de 2.048 bits para descifrar los parámetros actuales del RSA.

slide 7

Estado actual de la criptografía
Actualmente las investigaciones se centran más en resistir el ataque y más aún cuando se trata de la posibilidad de recibir ataques usando computadoras cuánticas, a esto se le conoce como criptografía post-cuántica en la que criptógrafos de todo el mundo han estado trabajando durante al menos una década para diseñar y mejorar los sistemas criptográficos de modo que sean resistentes a los ataques cuánticos

slide 8

¿Cuál es el peligro?
Los algoritmos cuánticos representan un peligro para la criptografía clásica; el más famoso y amenazante es el algoritmo de Shor ya que este resuelve el problema de factorización de enteros así como también el problema de logaritmos discretos en tiempo polinomial.
que básicamente estos conforman la base de la mayoría de los algoritmos criptográficos de clave pública.

esto podría ocasionar que los algoritmos clásicos de criptográfica puedan quedar virtualmente obsoletos. por otro lado lo único que nos impide hacer dichos ataques es una computadora cuántica lo suficientemente grande para poder realizarlos