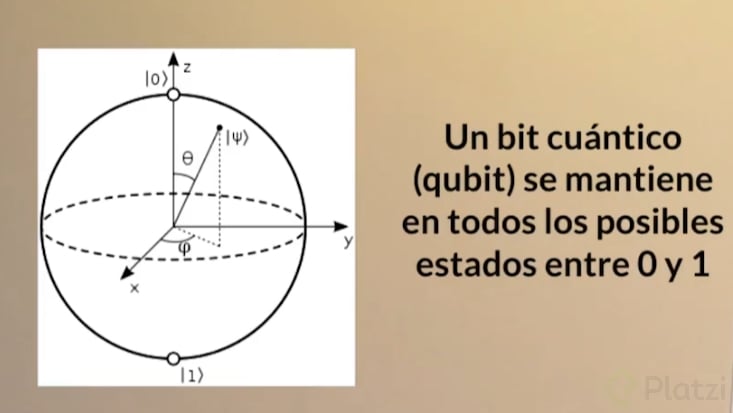
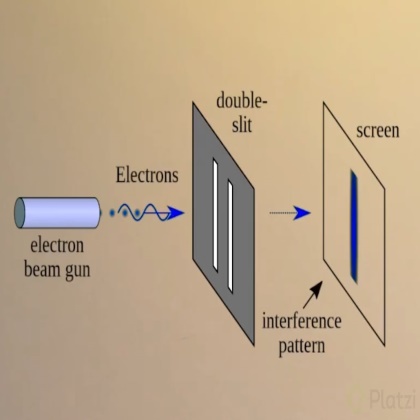
**Computación Cuántica**

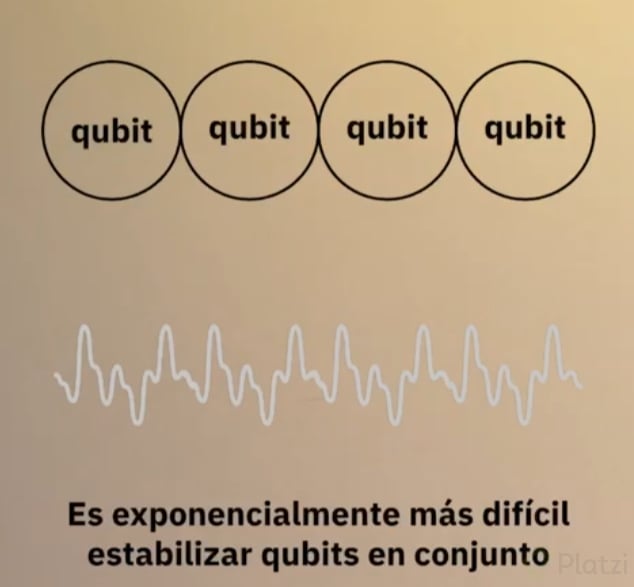
Uno de los temas de discusión respecto a la criptografia y su vigencia a largo plazo, es la computación cuantica ya que existe la creencia que con estos sistemas se podrian romper tambien criptosistemas ya que podemos violar algunas de las asunciones de seguridad computacional, sin embargo esto no es del todo cierto ya que la computación cuantica se ha enfocado a aplicaciones de investigación y menos en romper criptosistemas, si bien es cierto que se puede utilizar la computacion cuantica para estos propositos existen algunas limitaciones.

Por ejemplo el experimento de doble rendija, es un experimento que muestra las propiedades cuanticas cuando no se les esta observando, por lo que podriamos crear una representación cuantica de un bit, que llamaremos qubit, por lo que viene de quantum bit el cual se encontraria en una superposición de estados entre un cero y un uno, asi ajustar las propiedades del entorno y que el qubit resuelva el problema que le estamos dando.



El problema radica en que un qubit solo da valores entre 0 y 1 , ya que si nosotros queremos recopilar mas información o colocar mas qubits en conjunto estos se desestabilizan muy facilmente, debido a que tiene que estar en cero contacto con nada mas en el entorno, ya que si tenemos mas de un bite debemos asegurarnos que los qubit en conjunto interactuen de la forma que esperamos, lo que se da utilizando tecnologias de materiales muy especificas o muy bajas temperaturas.

Entonces se puede utilizar para paralelizar problemas como por ejemplo el computo del logaritmo discreto u otros problemas como factorizar numeros primos grandes, ya que utilizando estas técnicas podriamos en teoria romper el criptosistema  RSA , sin embargo estudios resientes han revelado que lo que necesario para resolver el problema de la factorización de numeros primos grandes es al rededor de un millon de qubits, pero a este nivel se vuelven tan inestables que es dificil mantenerlos en conjunto



A pesar que existen formas que son factibles en papel, en la practica son difíciles de replicar, adicionalmente existe listas y propiedades de los criptosistemas que garantizan resistencia a los sistemas cuanticos ya que hay problemas que son complejos de resolver aun utilizando una computadora cuantica.