12 MARZO 2021

II CONGRESO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Desafíos de la computación y criptografía cuánticas

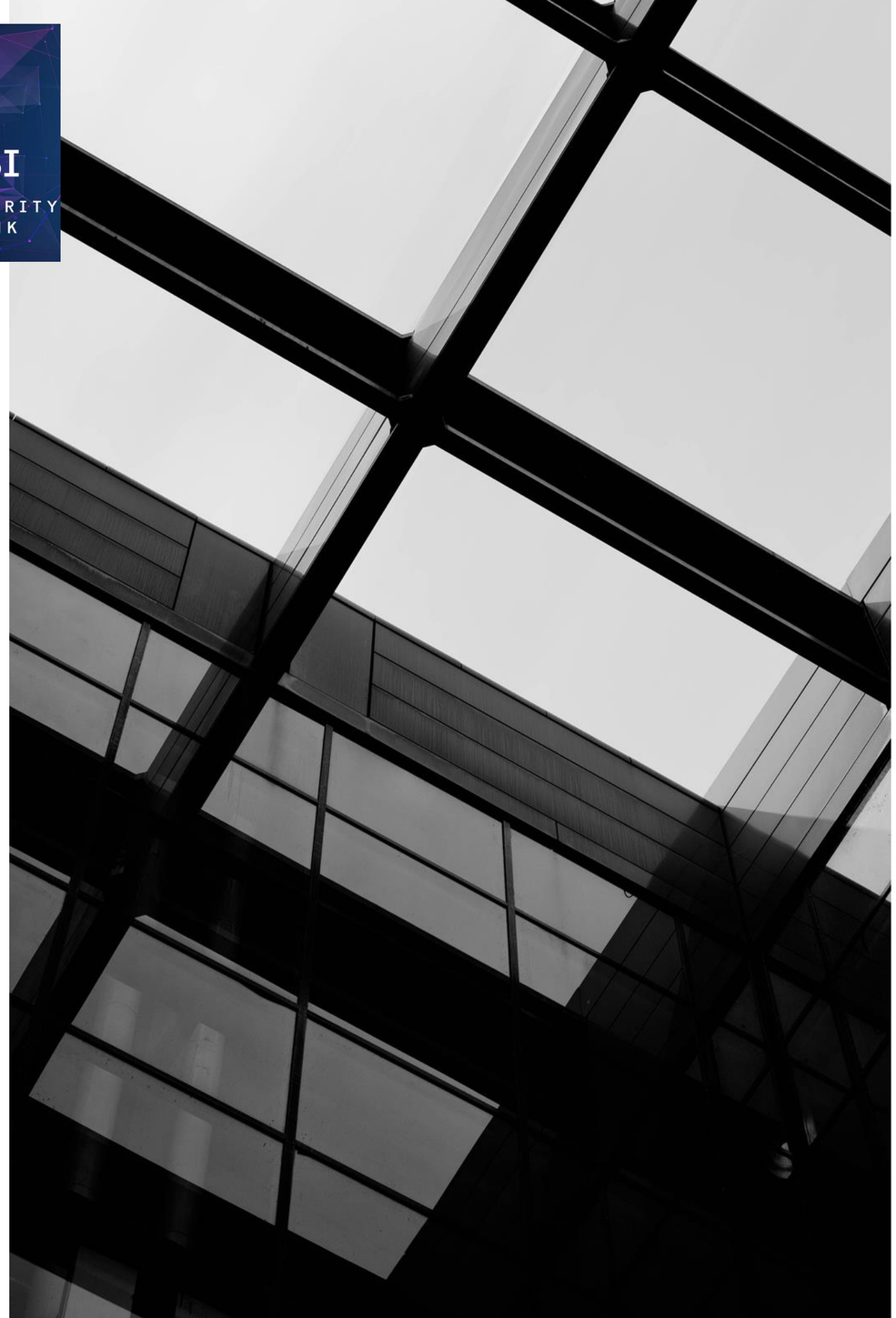
Speaker:
Haridas Umpierrez

Linkedin
www.linkedin.com/in/humpierrez

SOCHISI
DIGITAL SECURITY THINK TANK

CAPACITACIÓN USACH

SOCHISI.CL/ENVIVO



Tecnologías cuánticas

Tópicos

01 La barrera cuántica (breve historia de los bits)

02 Cubits

03 Computación cuántica

04 Criptografía cuántica

Clase de Ciencias Sociales XXXXXX

Algunas definiciones

Estado

Concepto matematico, que describe a un elemento cuántico, y entrega la densidad de probabilidad para los resultados de una medición. Los estados describen distintas propiedades del Sistema, por ejemplo la posición, el momentum, la energía, el spin, etc

$$|\varphi\rangle$$

Superposición

Los sistemas cuánticos pueden estar descritos por más de un estado (de la misma propiedad) a la vez. Por ejemplo, una partícula puede tener spin arriba y abajo al mismo tiempo, o existir en varios lugares a la vez.

$$|\varphi\rangle = a|\alpha\rangle + b|\beta\rangle$$

Entrelazamiento

Al tener mas de una partícula, el estado del sistema describe a las dos particulas a la vez, y esto hace que existan ciertas propiedades que dependan una de la otra, por ejemplo, dos electrones en un atomo tienen que tener spines opuestos, pero al mismo tiempo exsistir en superposición.

$$|\varphi\rangle + a|\alpha\beta\rangle + b|\mu\nu\rangle$$

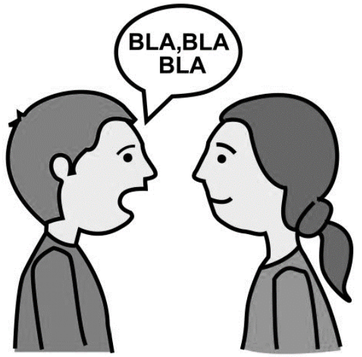
SOCHISI

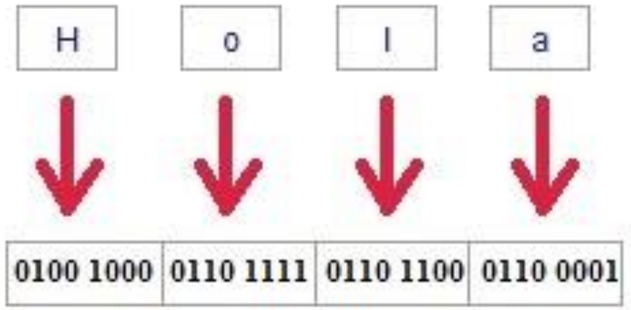
DIGITAL SECURITY THINK TANK

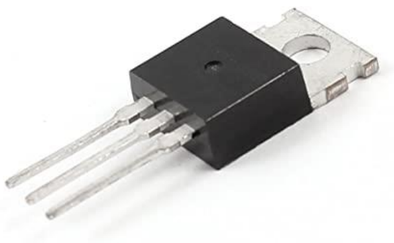
La barrera de lo cuántico

Codificación de la información

Históricamente, hemos codificado la información que requerimos guardar o procesar de una infinidad de maneras.







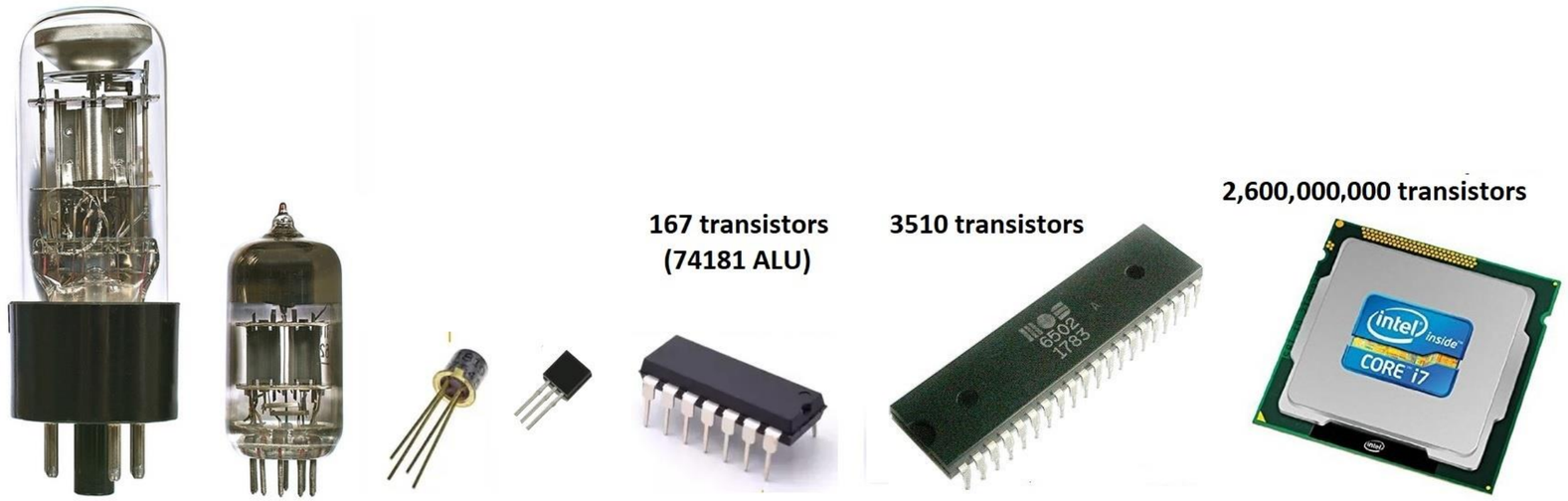
SOCHISI

DIGITAL SECURITY THINK TANK

La barrera de lo cuántico

Evolución de los Transistores

Es de conocimiento general, que la capacidad de computo aumenta a medida del tiempo, esto gracias a que cada vez se logran crear transistores más y más pequeños.



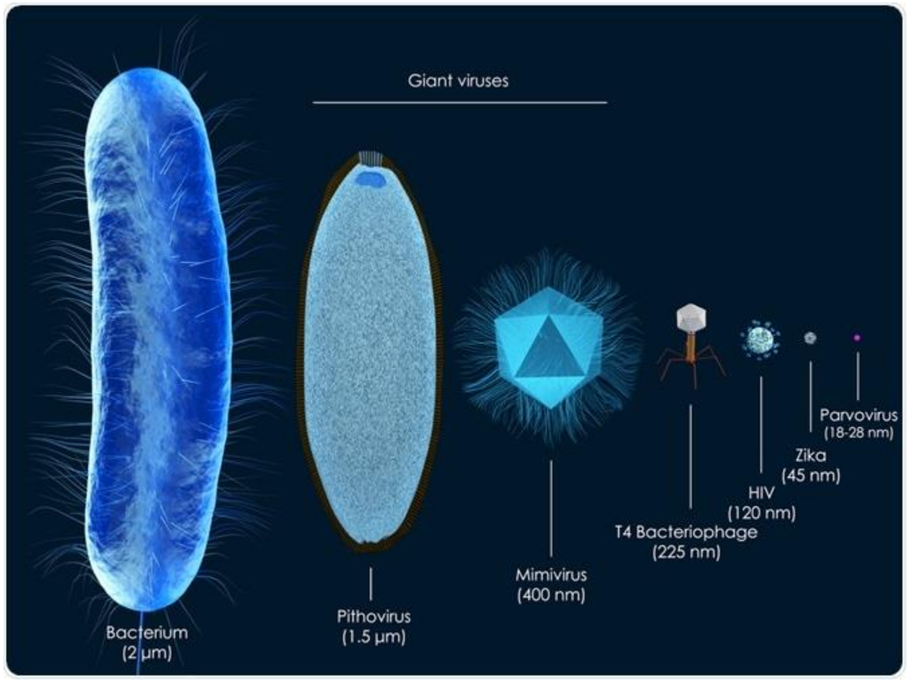
¿De que estamos hablando hoy?

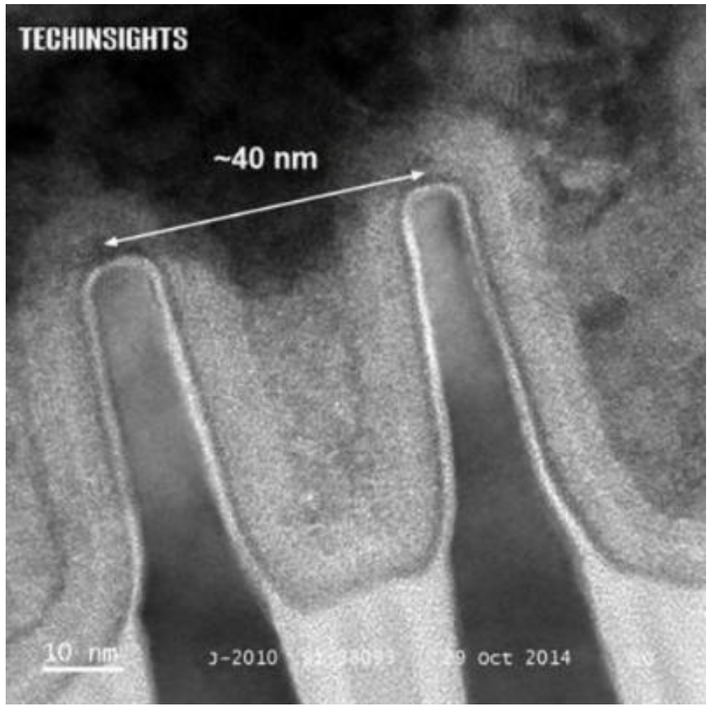
SOCHISI
DIGITAL SECURITY THINK TANK

La barrera de lo cuántico

A lo que hemos llegado!!

Hoy en día tenemos transistores de 5 nm de largo





$$1nm = \frac{1}{1000000000}m = 10^{-9}m$$

Clase de Ciencias Sociales Escuela Loma Alta

SOCHISI.CL/ENVIVO

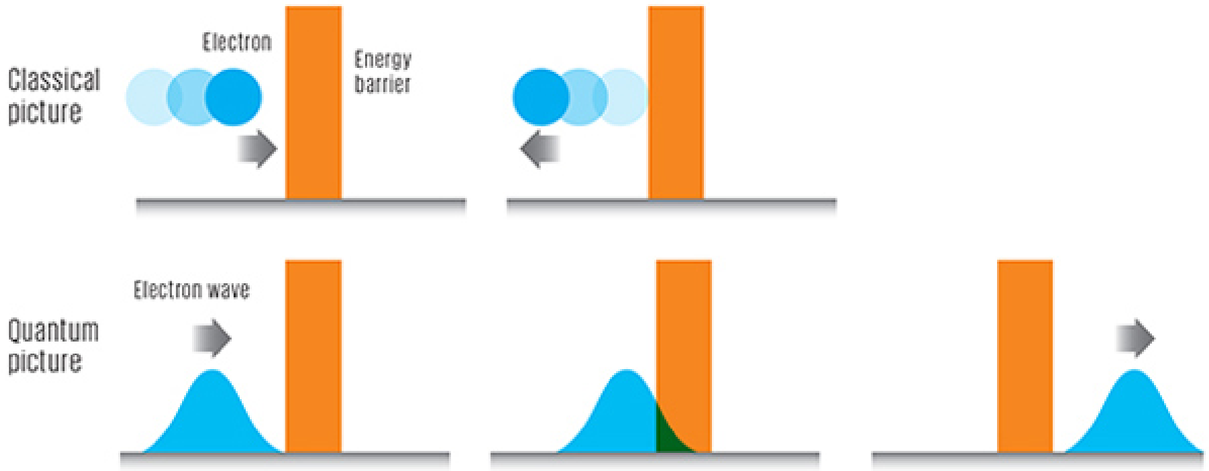
SOCHISI

DIGITAL SECURITY THINK TANK

La barrera de lo cuántico

Problemas con el Nanotransitor: Efecto de Tunel

Sin embargo, al llegar a tamaños atómicos, se comienzan a dar efectos cuánticos, en particular, tunneling.



Al ser tan pequeños los procesadores los electrones pasan de un transistor a otro aun cuando los canales están cerrados→ Se generan errores.

Clase de Ciencias Sociales Escuela Loma Alta

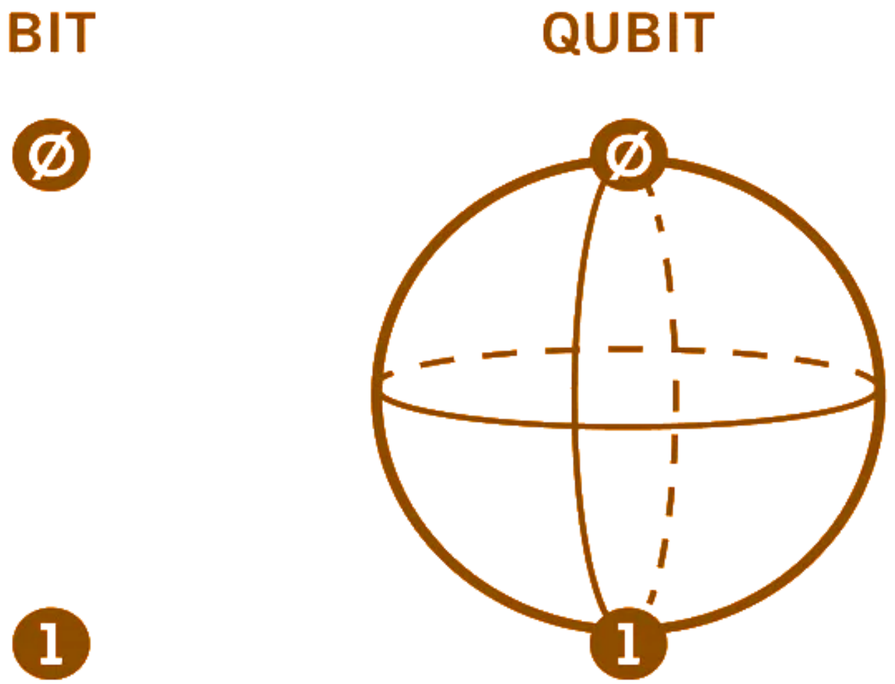
La barrera de lo cuántico

¿Es este entonces el limite de la computación?

SOCHISI
DIGITAL SECURITY
THINK TANK

El cubit

Supongamos una nueva manera de representar información

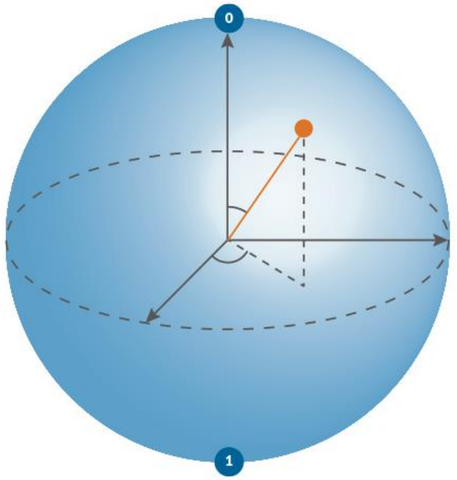


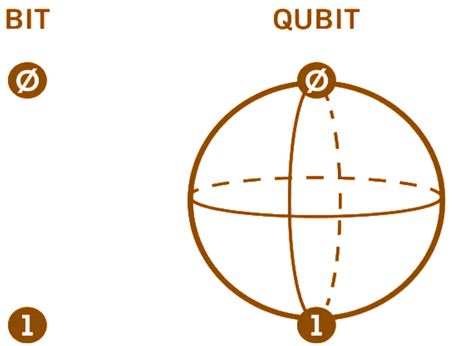
El cubit es una nueva manera de codificar información

El cubit

La superposición

Un cubit, es un sistema cuántico, que existe en un estado de superposición entre dos estados base. La elección de estos dos estados es arbitraria.





La superposición de un cubit existe justo hasta el momento antes de observarlo, al hacerlo, esta se rompe, y el cubit toma un valor determinado, por ejemplo, arriba (0) o abajo (1)

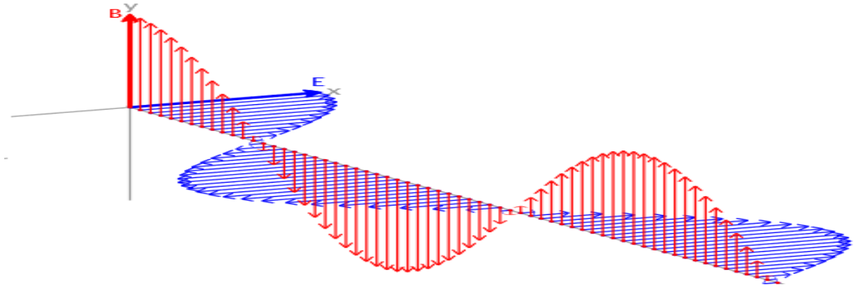
SOCHISI
DIGITAL SECURITY
THINK TANK

El cubit

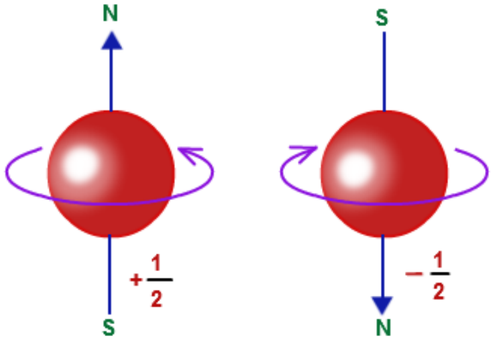
¿Cómo se construye un CUBIT?

No existe una manera estándar de construir un cubit, de la misma manera que un bit puede representarse físicamente de varias maneras.

Algunos ejemplos:



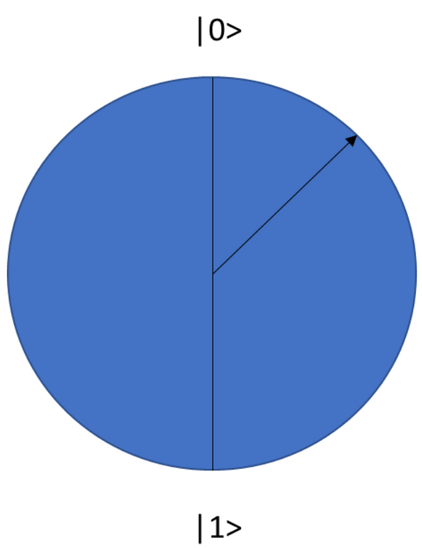
La polarización de un fotón

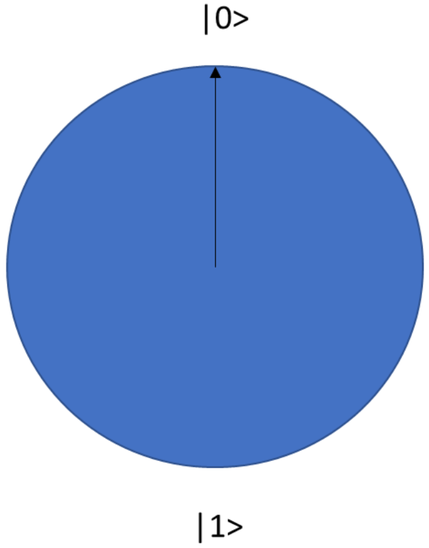


El spin de un electrón en un átomo

El cubit

Como se usa un CUBIT





$$|\phi> = a|0> + e^{i\varphi} b\ |1>$$

Aquí tengo un Cubit en estados de superposición.
¡No conozco su estado!

Al medirlo

$$|\phi'> = |0>$$

Obtengo uno de los estados que lo compone

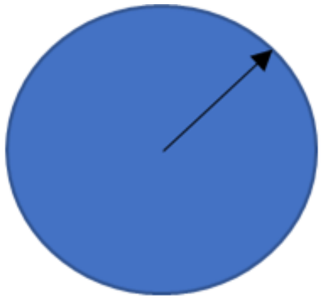
SE FUERZA A QUE DE INFORMACIÓN CONCRETA.

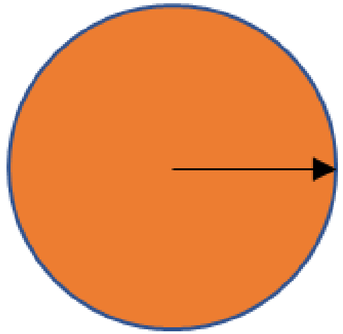
SOCHISI
DIGITAL SECURITY
THINK TANK

El cubit

Dependencia de la Medición

Mas interesante aún, el resultado no depende solo del cubit, si no de que medición se realice, si por ejemplo medimos en términos de otra combinación de estados





$$|\phi> = a|0_x> + e^{i\varphi}b\ |1_x>$$

Representemos al mismo CUBIT de otra manera

Pero elijo medirlo en otro eje

$$|\phi> = |0_x>$$

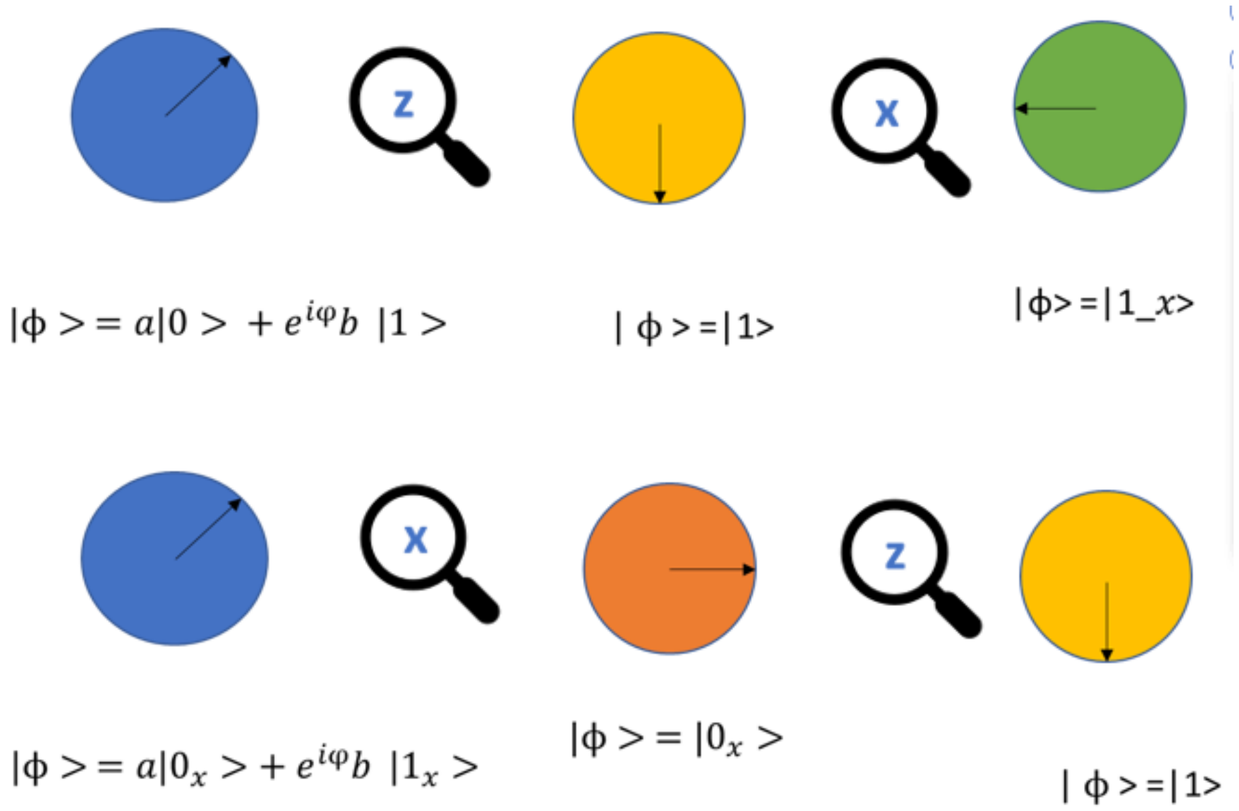
El resultado es se da en otro eje, siendo derecha o izquierda por ejemplo

SOCHISI
DIGITAL SECURITY THINK TANK

El cubit

Dependencia de la Medición

Vayamos un paso más adelante, supongamos que tenemos dos cubits idénticos, a los cuales voy a medir en los dos ejes, pero de manera invertida.



$|\phi> = a|0> + e^{i\varphi}b\ |1>$

$|\phi> = |1>$

$|\phi> = |1\_x>$

$|\phi> = a|0_x> + e^{i\varphi}b\ |1_x>$

$|\phi> = |0_x>$

$|\phi> = |1>$

El resultado es totalmente distinto, ¡SE PIERDE INFORMACIÓN!

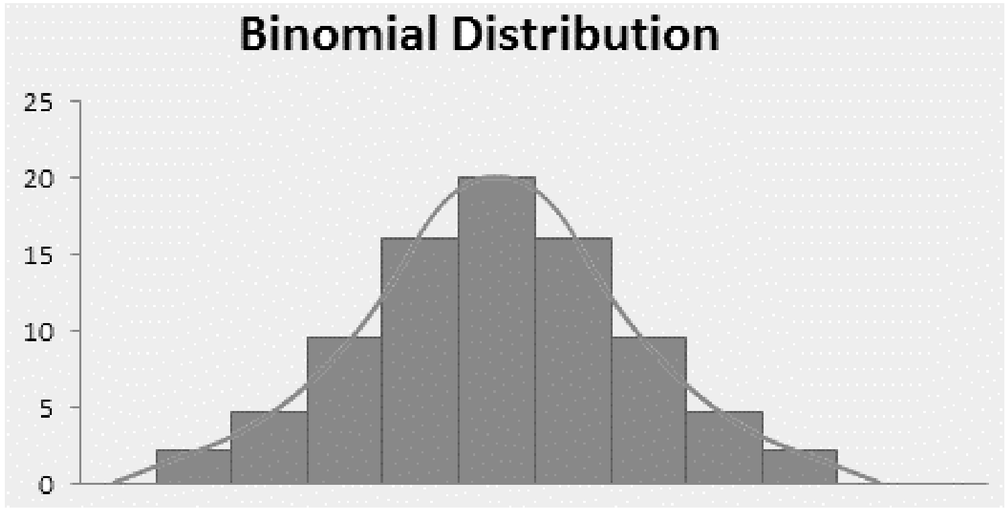
SOCHISI
DIGITAL SECURITY
THINK TANK

El cubit

Consideraciones sobre los CUBIT.

- Una propiedad interesante que resulta de la naturaleza probabilística de las mediciones de los cubits, es la generación de números genuinamente aleatorios.

- Esto eliminaría cualquier posibilidad de ataques que se basaran en encontrar patrones en los cifrados, aumentando la seguridad de éstos.



El cubit

¿Cómo el cubit viene a revolucionar las tecnologías?

SOCHISI

DIGITAL SECURITY THINK TANK

Computación cuántica

¿Qué es un computador cuántico?

Un computador cuántico, es una maquina que utiliza fenómenos cuánticos para almacenar y procesar datos.

Los procesadores de los computadores cuánticos, están conformados por cubits entrelazados.

Clase de Ciencias Sociales Escuela Loma Alta

SOCHISI
DIGITAL SECURITY
THINK TANK

Computación cuántica

¿Como se construye un computador cuántico?

No existe una manera estándar de construir un computador cuántico, o incluso de construir un procesador.

La manera en la que las maquinas se comunican con los cubit dependen totalmente de cual es la elección de construcción del chip de cubits en si.

Algunos ejemplos de procesadores:

- Chips de silicio
- Chips superconductores
- Trampas de iones
- Materiales topologicos

Computación cuántica

Dentro de los chips

El estado cuántico de un computador cuántico de dos cubits se ve como

$$|\phi> = a_1|00> + a_2|10> + a_3|01> + a_4|11>$$

En donde se tienen cuatro bits codificables

De manera similar, uno con tres cubits se ve como

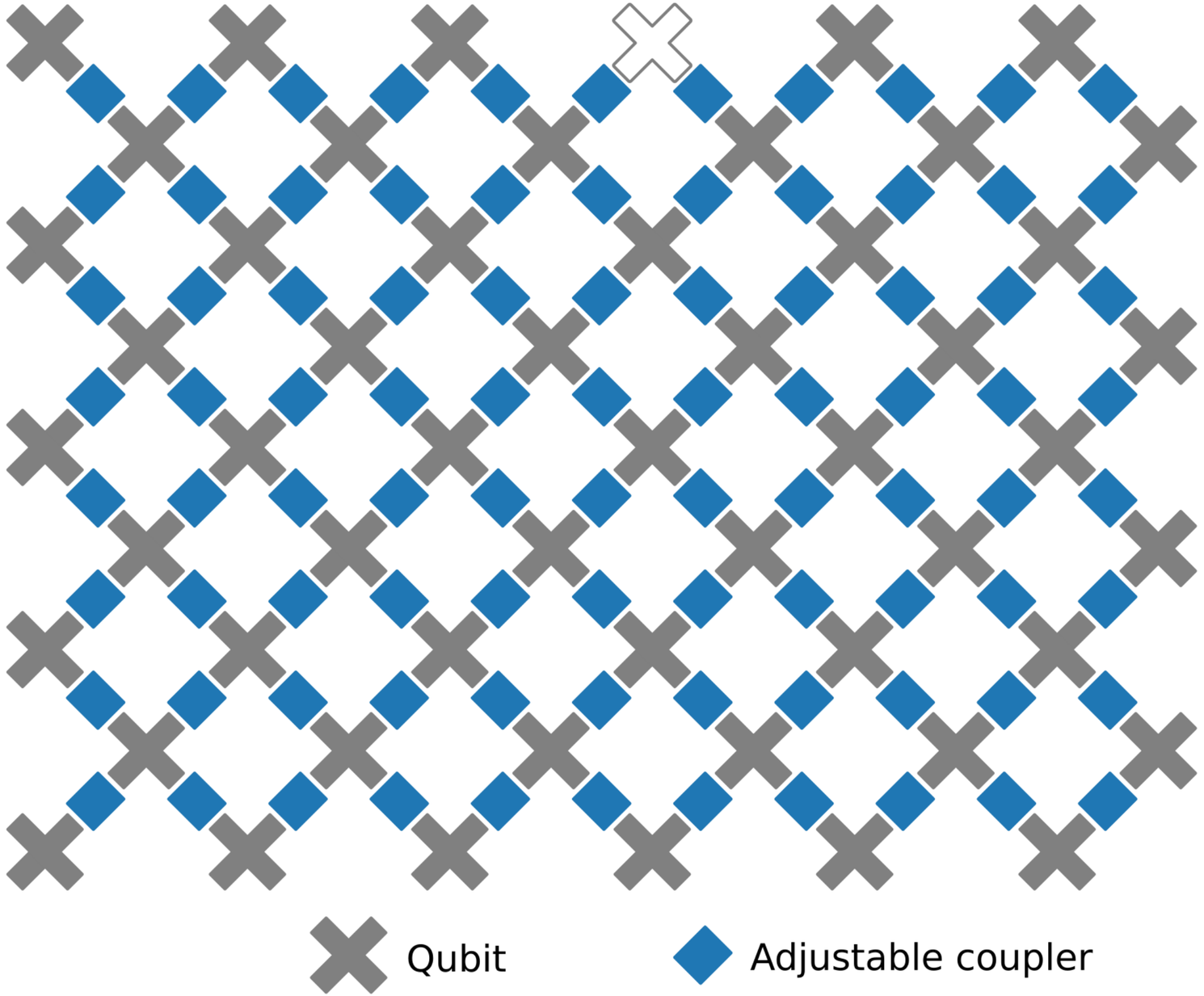
$$|\phi> = a_1|000> + a_2|001> + a_3|010> + a_4|011> + a_5|100> + a_6|101> + a_7|110> + a_8|111>$$

Donde ahora se tienen ocho bits codificables

SOCHISI

DIGITAL SECURITY THINK TANK

Computación cuántica



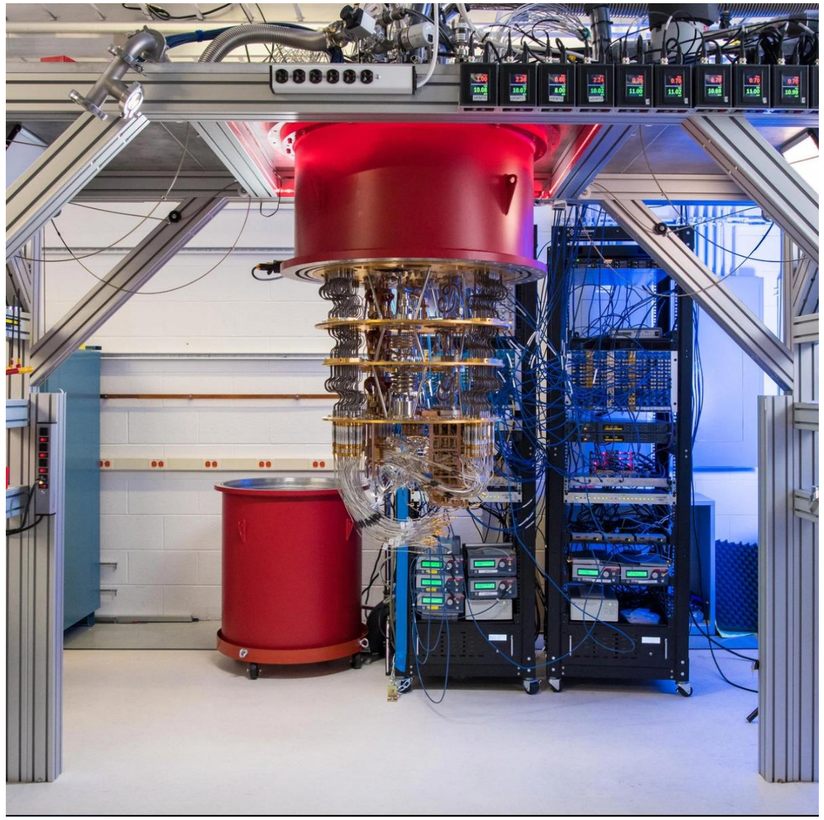
Clase de Ciencias Sociales Escuela Loma Alta

SOCHISI
DIGITAL SECURITY THINK TANK

Computación cuántica

Fuera del chip

Por las necesidades de los procesadores, los computadores cuánticos utilizan grandes volúmenes.



Computador cuántico de Google

- Deben estar a muy baja temperatura
- Deben estar asilados del “universo”

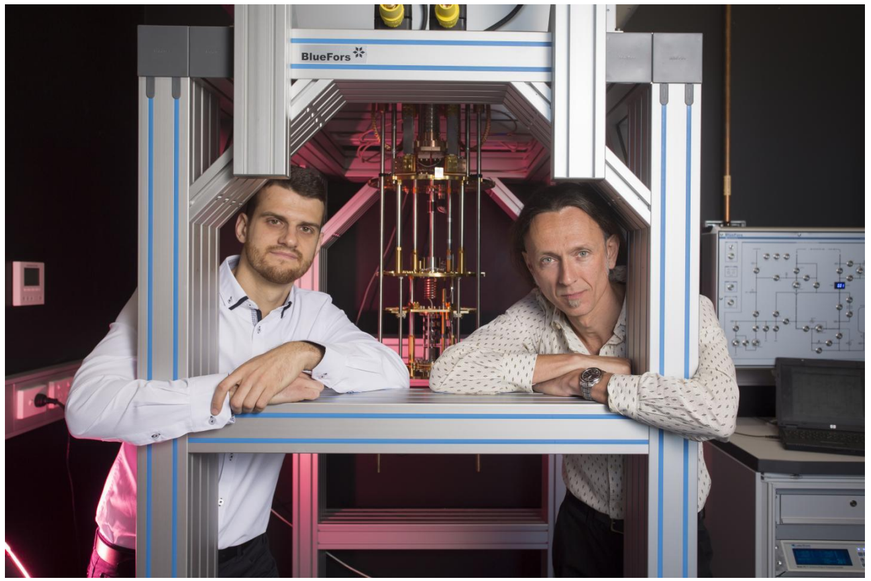
SOCHISI

DIGITAL SECURITY THINK TANK

Computación cuántica

Otros ejemplos de Computadores Cuanticos

Computador cuántico de IBM

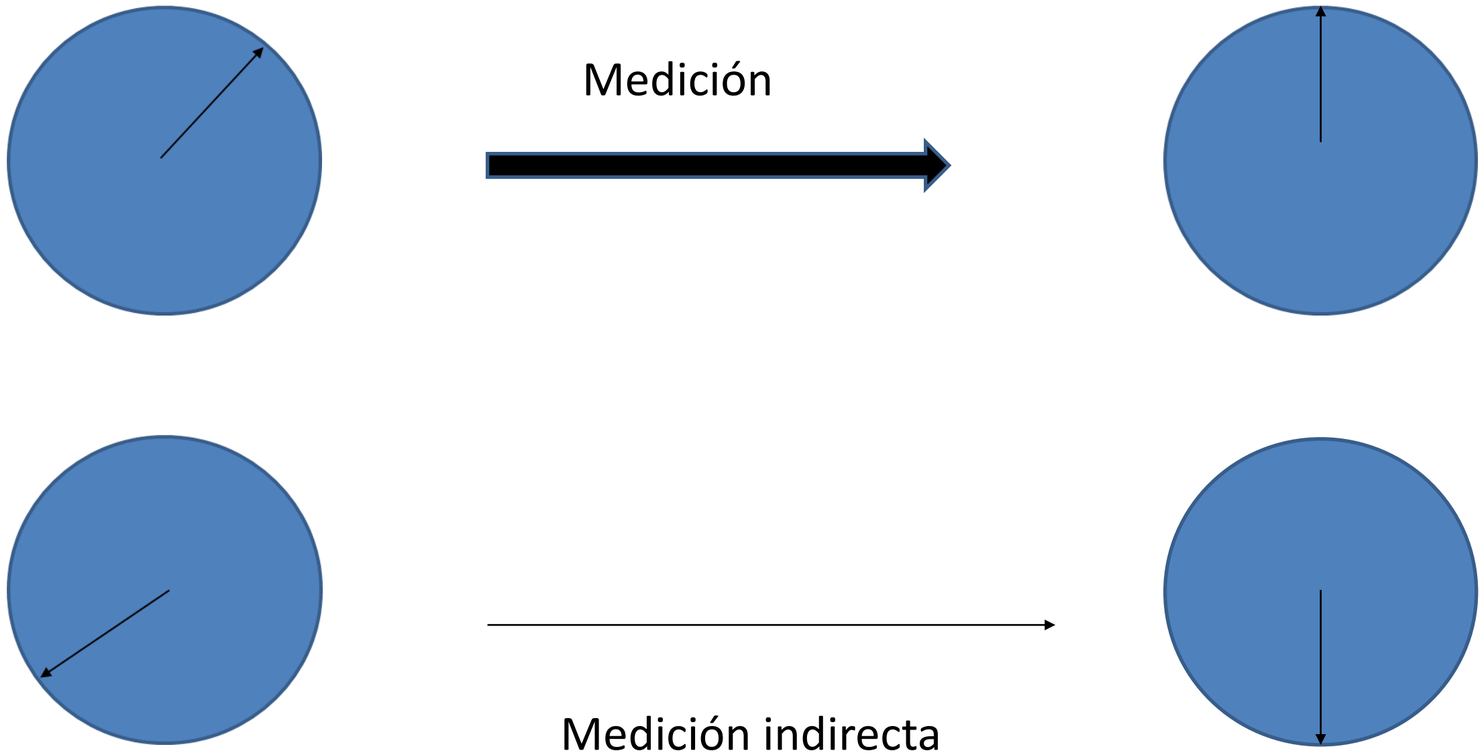


Computador cuántico Dr. Andrea Morello

Computación cuántica

¿Cómo funcionan?

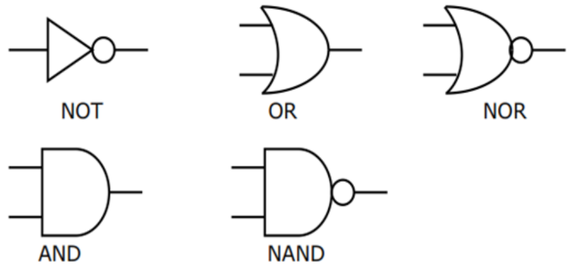
Debido a que los cubits en un chip están entrelazados, hacer una operación sobre uno de los cubits afecta a todo el sistema.



Computación cuántica

Puertas lógicas cuánticas

De la misma manera que en computación clásica se tienen puertas lógicas, en computación cuántica se tienen puertas cuánticas



Descripción	Puerta cuántica	Matriz unitaria
Trasformación identidad	|0> → |0> I: |1> → |1>	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$
Negación	|0> → |1> X: |1> → |0>	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$
Y=ZX, combinación de ambas	|0> →-|1> Y: |1> → |0>	$\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}$
Z es una operación de cambio de fase	|0> → |0> I: |1> → -|1>	$\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$

- Puerta lógica de Hadamard

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

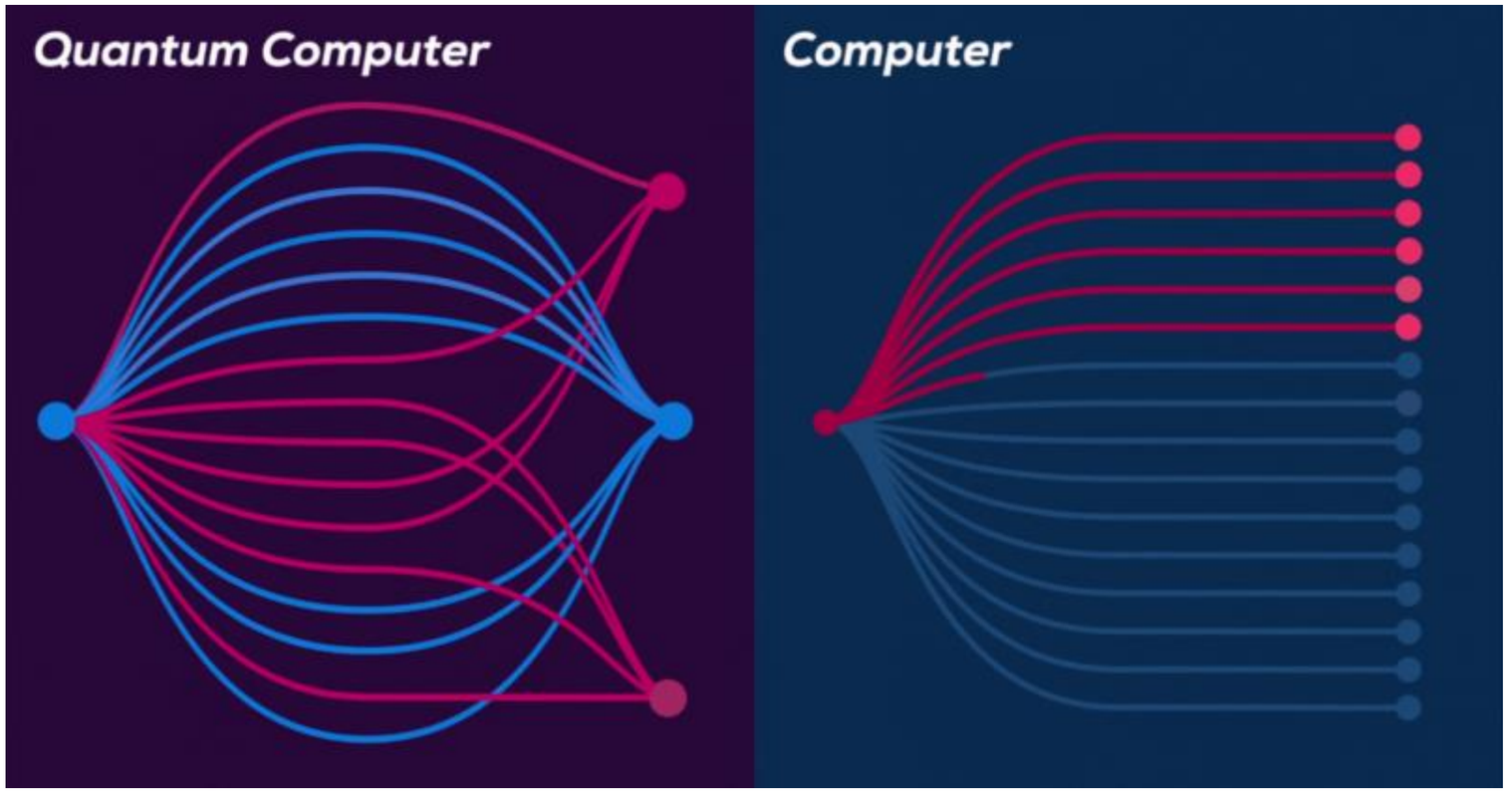
$$H = H^{-1} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$$

SOCHISI
DIGITAL SECURITY THINK TANK

Computación cuántica

Capacidad de cómputo

La ventaja es que se puede llevar al estado de tal manera que se puedan hacer mediciones de manera paralela para obtener varios estados distintos, lo que aumenta dramáticamente la velocidad de procesamiento.

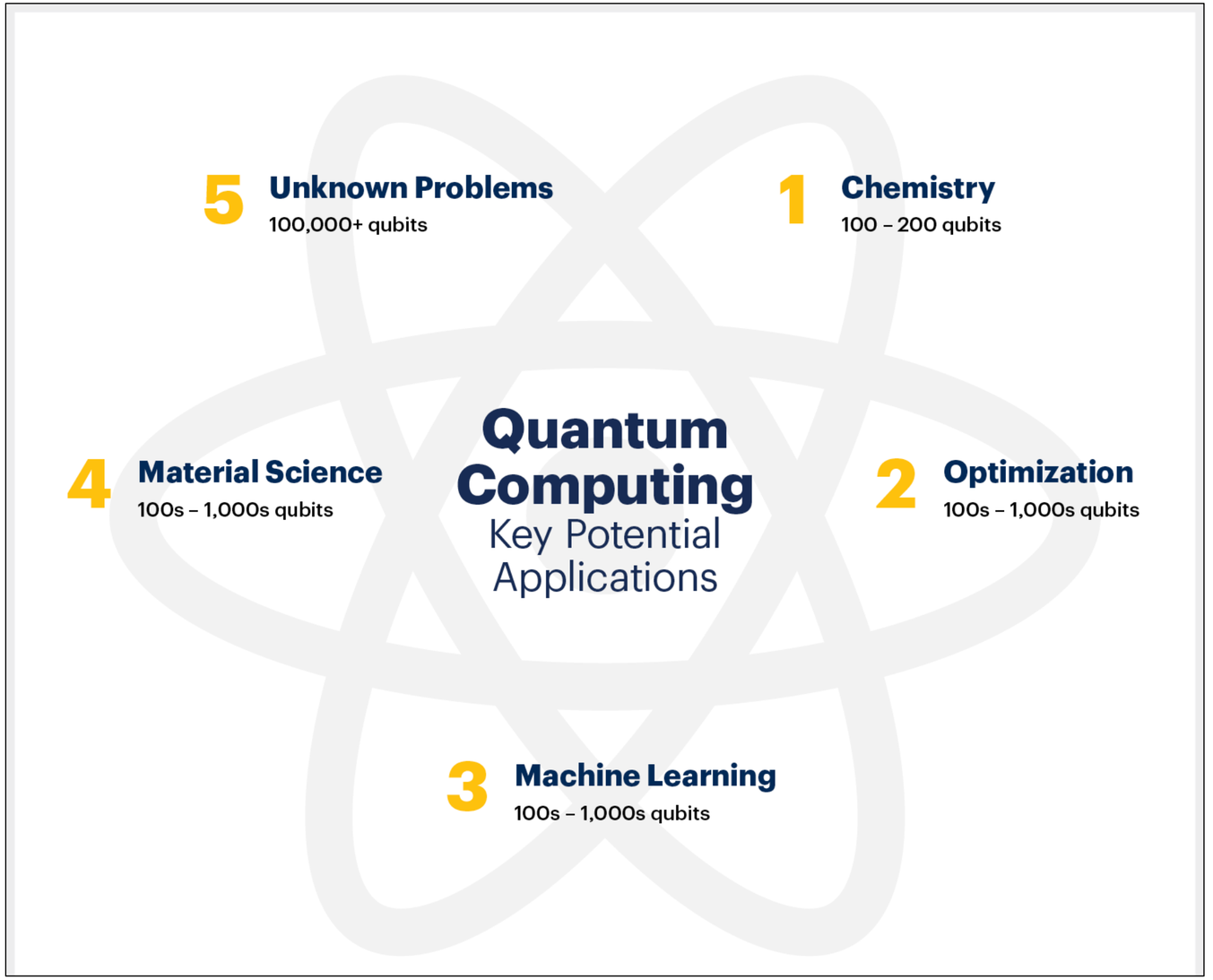


SOCHISI

DIGITAL SECURITY THINK TANK

Computación cuántica

Potencial de la Computación Cuantica - Gartner



Clase de Ciencias Sociales Escuela Loma Alta

Computación cuántica

Estado actual de la computación cuántica

Actualmente IBM posee el computador cuántico con más cubits, con un total de 65 cubits.

Le sigue el computador de Google, con 53(54) cubits, el cual, en 2019 logró la “supremacía cuántica”, resolviendo un problema que a un supercomputador le llevaría 10.000 años en solo 200 segundos.

Sin embargo, aún no se han resuelto problemas útiles en un computador cuántico mejor que en uno clásico.

Computación cuántica

¿Los computadores cuánticos reemplazarán a los computadores clásicos?

NO

(probablemente)

Problemas a resolver

- Estandarización de su construcción (reinventar el transistor)
- Reducción de ruido
- Total entrelazamiento
- Decoherencia

SOCHISI

DIGITAL SECURITY THINK TANK

Computación cuántica

Pero no todo es positivo.

Los computadores cuánticos reducen la complejidad de un problema exponencial, como la factorización en RSA, a un problema polinomial

$$2^{N^{\frac{1}{3}}} \rightarrow N^3$$

En la realidad, para descifrar un numero de 2000 bits, se requieren alrededor de 400.000 cubits físicos.

Por otro lado, existen algoritmos teorizados que están diseñados para operar en un computador cuántico, tales como el algoritmo de Shor, el cual permitiría factorizar un numero en sus factores primos con solo 100 cubits perfectamente entrelazados.

Computación cuántica

¿Cómo nos defendemos de esto?

SOCHISI

DIGITAL SECURITY THINK TANK

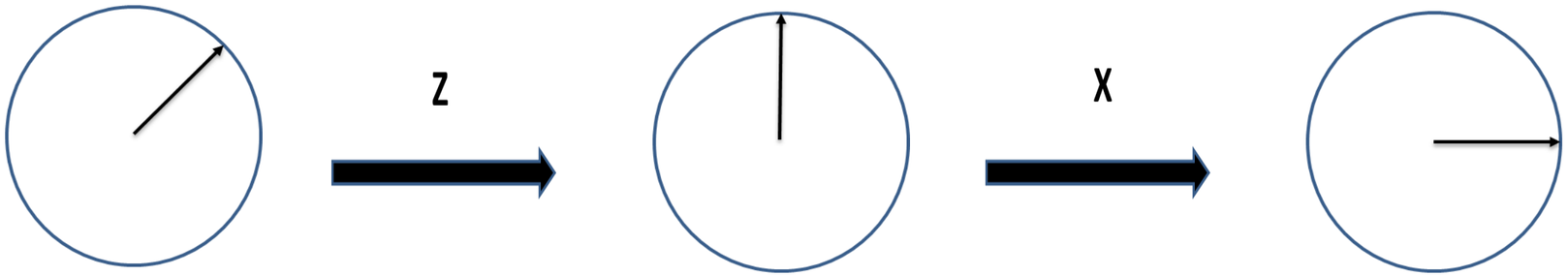
Criptografía cuántica

Criptografía cuántica

¿Qué es la criptografía cuántica?

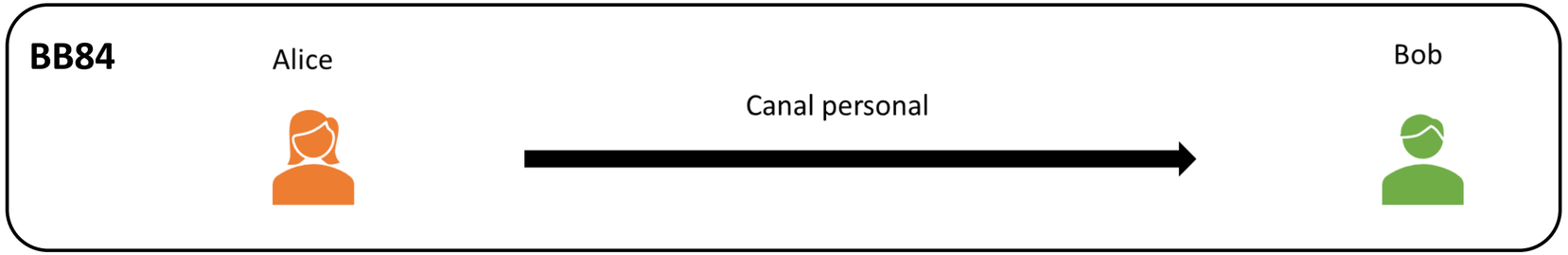
Mas conocida como Distribución de Llaves Cuánticas (QKD), son protocolos que aprovechan las propiedades de los cubits para codificar bits en cubits y luego generar y distribuir claves de cifrado simétricas asegurando al integridad incondicional del canal privado.

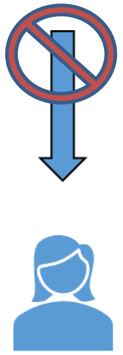
QKD se basa principalmente en el hecho de que medir un cubit altera permanentemente la información contenida en éste.



Criptografía cuántica

De esta manera, cualquier intento por parte de un tercero de hacerse con la clave sería identificado, manteniendo a la clave en total secreto, impidiendo ataques como los que se podrían realizar con un computador cuántico sobre un protocolo RSA.



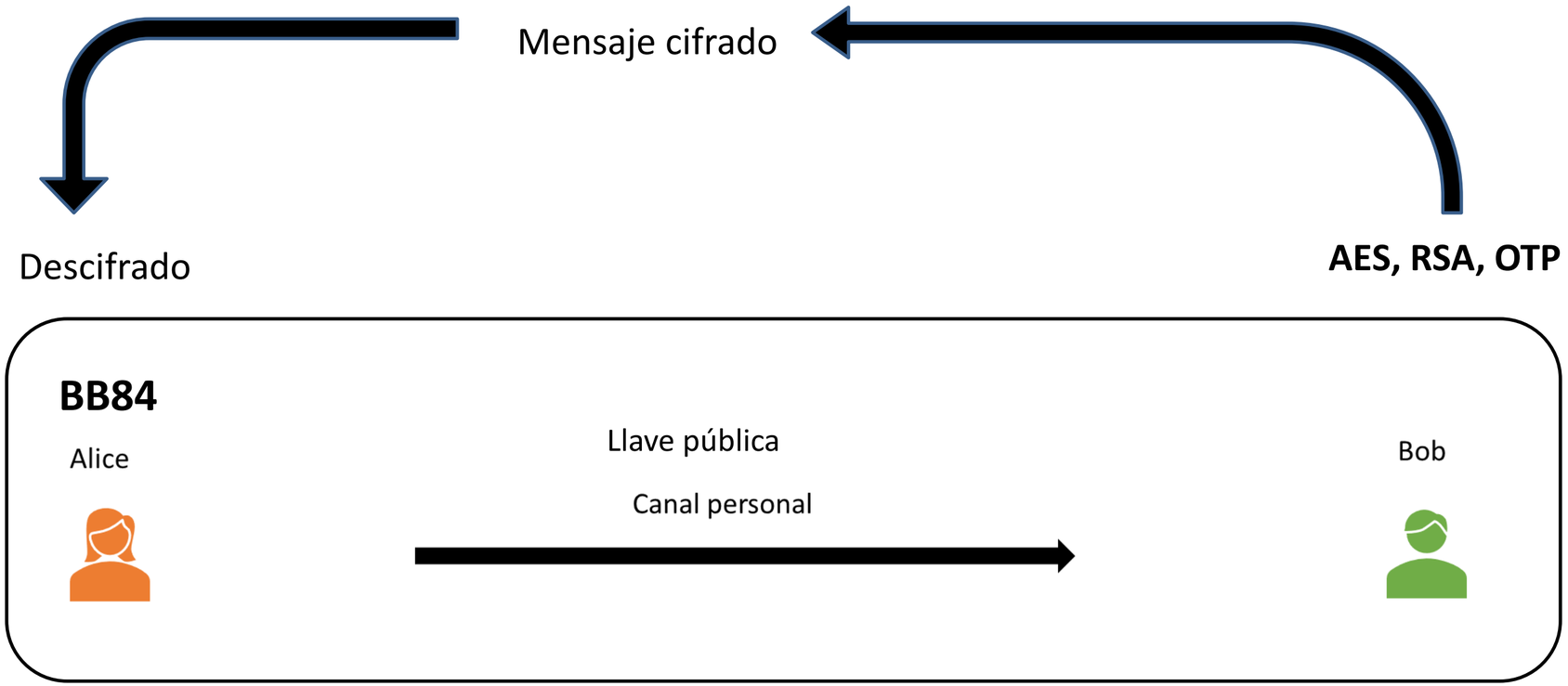


SOCHISI
DIGITAL SECURITY THINK TANK

Criptografía cuántica

Objetivos

Un hecho importante a mencionar, es que QKD se limita a generar y distribuir llaves públicas. El cifrado y la transmisión del mensaje se realizan mediante protocolos preexistentes, tales como AES, RSA o lo más usado, libretas de un solo uso.



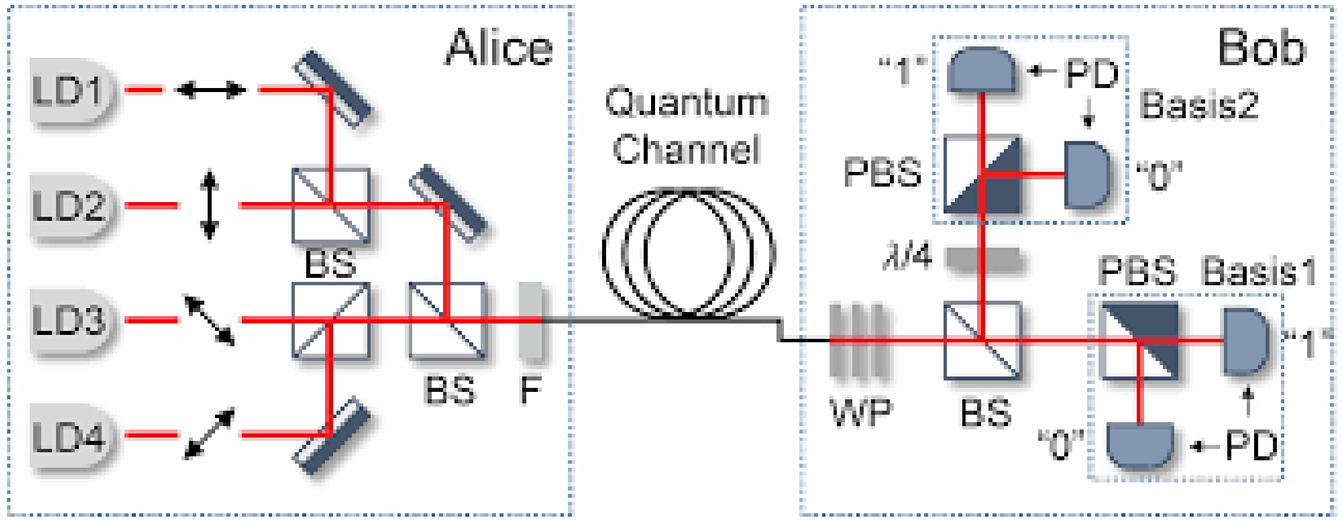
SOCHISI
DIGITAL SECURITY THINK TANK

Criptografía cuántica

¿Qué utilizan?

A diferencia de lo que se podría creer, los protocolos de QKD NO requieren de un computador cuántico. Su implementación es relativamente sencilla.

En general, se requiere un computador que genere una cadena binaria y un aparato, por lo general un emisor de fotones, que codifica la cadena en una serie de cubits, representados por fotones con polarizaciones controladas.



Criptografía cuántica

Es por esto que actualmente existen diversas compañías que aplican soluciones de criptografía cuántica, no solo en forma de QKD, si no que además en soluciones que generen cadenas verdaderamente aleatorias.

Algunas compañías que ofrecen soluciones son:

- Quantum numbers corp
- Kets
- Cryptonext security
- FlipsCloud
- Sixscape

Criptografía cuántica

Ventajas

- Resistente a computación cuántica
- Mínimo filtrado de información
- Fácil de implementar

Problemas

- Limitantes tecnológicas
  - Distancia de comunicación
  - Perdida de información
  - No son infalibles a todos los ataques

Conlcusiones

En resumen

- Las tecnologías cuánticas se han vuelto más relevantes que nunca.
- La ciberseguridad se mantiene a salvo.
- Es necesaria una articulación más fuerte entre las disciplinas de ciberseguridad y física.
- Además de una complementación de la formación actual de ciberseguridad con las nuevas tecnologías cuánticas.

12 MARZO 2021

II CONGRESO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

¡Muchas Gracias!

Desafíos de la computación y la criptografía cuanticas

SOCHISI
DIGITAL SECURITY THINK TANK

Speaker:
Haridas Umpierrez

Linkedin
Haridas Umpierrez Neumann

CAPACITACIÓN USACH

SOCHISI.CL/ENVIVO