INTRO

- QUBITS
- OPERADORES CUÁNTICOS
- TEOREMA DE NO CLONACIÓN
- ENTRELAZAMIENTO CUÁNTICO Y NO LOCALIDAD
- APLICACIONES
- CODIFICACIÓN CONJUGADA
- DISTRIBUCIÓN CUÁNTICA DE CLAVES
- BIT COMMITMENT IMPLICA OBLIVIOUS TRANSFER
- MODELOS DE ALMACENAMIENTO CUÁNTICO LIMITADO
- COMPUTACIÓN CUÁNTICA DELEGADA
- COIN FLIPPING
- LIMITACIONES Y RETOS

Qubits

Del mismo modo que un bit binario es la unidad básica de información en la computación clásica (o tradicional), un qubit (o bit cuántico) es la unidad básica de información en la computación cuántica.
Un qubit logra una combinación lineal de dos estados. Un bit binario clásico sólo puede representar un único valor binario, como 0 o 1, lo que significa que solo puede estar en uno de dos estados posibles.
Podemos escribir cualquier estado en un qubit como $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, donde los estados $|0\rangle$ y $|1\rangle$ forman una base para el espacio vectorial bidimensional, y donde α y β son números complejos

Teorema de no clonación

Una de las propiedades más fundamentales de la información cuántica es que no es físicamente crear una copia idéntica de un estado cuántico, es decir, no hay proceso físico que tome como entrada un único sistema cuántico (por ejemplo un fotón) y como salida de dos copias idénticas, vamos a demostrarlo con una reducción a lo absurdo.

Operadores cuánticos:

Un sistema cuántico se describen mediante operaciones lineales, formalmente estas operaciones se pueden expresar como matrices complejas y se describen como circuitos, que consisten en puerta cuánticas básicas:

- Negación X: invierte/niega los 0 y 1
- Phase Z: cambia la fase del sistema, es decir, invierte el signo de los vectores
- Hadamard H: es una operación de modelizar, es decir, pasar a un estado rotado (pasar de una base a otra)
El resto de operadores son combinaciones de los operadores unitarias,
Para 2 o más fotones, una de la más importante a destacar es el operador CNOT -> invierte si el primer fotón es 1, solo cuando el primero es 1 (fotón de control) y invierte el segundo fotón

Bit commitment no es fiable es cuántica pero sí en clásica, en algunos papers actuales se empiezan a vislumbrar algo.

Entrelazamiento cuántico y no localidad

En general un sistema de 2 fotones (qubits en nuestro caso) no se puede describir cada qubit individualmente.

Entrelazamiento cuántico: Es un fenómeno cuántico (predicho por Einsten, Podolsky y Rosen) sin equivalente en el mundo clásico, en el cual se estipula que los estados cuánticos de dos o más objetos (como por ejemplo fotones) se deben describir mediante un único estado que involucra a todos los demás objetos del sistema entre sí, esto es así aunque los objetos estén separados espacialmente. Ejemplificamos esto con un ejemplo, podemos imaginar a Alice y Bob con dos qubits (por ejemplo unos fotones), Alice decide medir su qubit, como resultado de la medición su qubit colapsa y produce un estado cualquiera, con el entrelazamiento cuántico, al mismo tiempo que el qubit de Alice se media, el sistema de Bob produce el mismo resultado y aunque esto ocurre simultáneamente en ningún momento el sistema ha enviado información de Alice a Bob. Únicamente el sistema proporciona a Alice y Bob un bit aleatorio compartido. Estas correlaciones son más fuertes que todas las correlaciones que podrían obtener al compartir solo aleatoriedad clásica ya que violan de mayor manera la **desigualdad de Bell**, demostrando que el mundo se describe con mayor precisión con la mecánica cuántica que con la mecánica clásica.

Si pensamos en el entrelazamiento cuántico no podemos evitar pensar que este principio viola el principio de la localidad, en el cual se establece que dos objetos suficientemente alejados uno del otro no pueden influirse mutuamente de manera instantánea y simplemente los objetos sólo podrían verse influidos por su entorno.

Aplicaciones

Esta teoría es sin duda la teoría física más exitosa y probada de todos los tiempos; describe una amplia gama de sistemas físicos y, por lo tanto, ofrece una gran cantidad de posibles sistemas físicos que pueden servir como dispositivos cuánticos. Estas posibilidades

incluyen computación cuántica fotónica, qubits de superconducción, resonancia magnética nuclear, computación cuántica con trampa de iones y computación cuántica atómica

Codificacion Conjugada

La codificación conjugada está basada en el principio de que podemos codificar la información clásica en bases cuánticas conjugadas. Este hecho es tán importante como que la mayoría de protocolos en la criptografía cuántica aprovechan la codificación conjugada.. El principio es básico, para simplificar la presentación asociaremos un qubit con un fotón y la polaridad de este como un grado cuántico de libertad. Entre otros el qubit se puede polarizar, horizontalmente, verticalmente, diagonal para la derecha / o diagonal para la izquierda \. Esto es una propiedad cuántica y podemos asociar Horizontal = |0, Vertical =|1,

$|\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\swarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, y realizar operaciones cuánticas en estos estados.

Bases conjugadas:
Base rectilínea= horizontal, vertical
Base Diagonal = diagonal
La relevancia de la codificación conjugada en la criptografía cuántica se resume en dos funcionalidades clave

1. Medir en una base destruye irrevocablemente toda información sobre la codificación en su base conjugada.
2. El generador de la codificación cuántica puede verificar su autenticidad, sin embargo, sin conocimiento de la base de codificación, y dado el acceso a un único estado codificado, ningún tercero puede crear dos estados cuánticos que pasen el procedimiento de verificación con alta probabilidad

Distribución Cuántica de Claves

Este es el uso más exitoso y útil en la actualidad. El QKD o protocolo BB84, consiste en el intercambio de clave entre dos usuarios por ejemplo, Alicia y Bob. Alicia toma una serie de ceros y unos, y los codifica utilizando una de las dos bases de forma aleatoria con cada bit:

↕ ↗ ↕ ↔ ↘ ↔ ↘ ↘ ↗ ↕ ↘ ↕ ↘
0 1 1 1 0 1 1 1 1 0 0 0 1

Bob recibe ceros y unos polarizando cambiando también la base con cada bit de forma aleatoria, lo cual hace que Bob obtenga el bit correcto si usa la base correcta, y si no tenga un 50% de posibilidades de que salga 0 o 1 en los que la base es distinta a la que Alicia ha usado, esto ocurre gracias al principio de las bases conjugadas que hemos visto antes. Cuando ya ha medido todos los fotones, le envía a Alicia la secuencia de polarizadores usada en la medición: R D R R D R D D D R D R D
y Alicia la compara con su secuencia, y le dice cuál ha usado correctamente y cual no.

La parte correcta será la clave que ambos usarán si no ha habido un alto nivel de errores, para encriptar y desencriptar la información que desean compartir. La encriptación será igual que las hasta ahora vistas en clase, pero la clave ya no será tan sencilla de obtener. ESTO ES SOLO INTERCAMBIO DE CLAVES

Una vez se han quedado con los valores correctos, para comprobar el nivel de errores, por ejemplo por ternas de datos, si la suma de los correctos es par o impar, y si supera un umbral determinado se considerará que habrá alguien observando la comunicación y no se usará esa clave.

Por las propiedades previamente explicadas, si alguien intercepta el mensaje, no solo no sabrá que es correcto, sino además, enviará la clave a Bob modificada ya que al observarlo está perturbando sus estado cuántico, por lo que Bob y Alicia se darán cuenta de que hay un Man-In-The-Middle observando la comunicación.

Es vital que la clave se comparta, por el medio que sea (ambiente, fibra óptica, etc), pero siempre de forma lineal, de fotón en fotón, ya que si enviásemos un haz de luz con información habría cientos de fotones iguales que, al alterar solo unos pocos, no pasaría nada, pero si enviamos una única línea de fotones, como hemos dicho antes con el principio de no clonación, con cada fotón alterado, aumenta la posibilidad de detectar al MITM, hasta que esta posibilidad alcance fácilmente el 99,99%. Esto se comprueba reenviando Bob fotones polarizados como Alicia le ha dicho que es correcto, y si Alicia recibe correctamente los Qubits, entonces no habrá problema, pero por cada fotón que Alicia polarice recibiendo un valor erróneo, comenzará a aumentar las posibilidades de que hayan interceptado la clave.

Existe un protocolo de BB84 mejorado que, en pocas palabras, aplica el entrelazamiento cuántico, enviando a Alicia un Qubit y a Bob otro, pero este último con delay, y los resultados que lleguen a Alicia, le llegarán exactamente igual a Bob.

Bit comprometido implica oblivious transfer

OT y BC son dos pilares para la criptografía.
Wiesner introduce una manera de enviar dos mensajes que luego fue redescubierto. En OT Alice manda dos mensajes, Bob recibe uno solo, esto es seguridad para ambos, ya que Bob solo recibe un bit dependiendo de su bit c y Alicia no puede aprender nada sobre la elección de Bob. La importancia de OT es el hecho de que es universal para asegurar la computación bipartida. Esto es un indicador excelente del poder criptográfico de un modelo.

El BC consiste en asegurar la siguiente funcionalidad bipartida, Alice no puede cambiar un bit que ha entregado a Bob y este no podrá verlo hasta que Alice no le envíe la clave.

Protocolo cuántico para la OT de Bennett, Brassard, Crépeau, and Skubiszewska
Ellos sugirieron que Alice mandase dos mensajes y bob eligiera uno dependiendo de su bit c. Bob guarde dos listas de bit tras comprobar con Alice las bases, en una lista guarda los bits bien leídos en I_c y los errores en I_1-c e informa a Alice de I_0 y I_1 sin saber donde están los correctos o los errores. Por último Alice creará dos funciones hash mapeando

desde n/2 hasta 1 bit y enviará $s_i = f_i(x|_{I_i}) \oplus m_i \text{ for } i = 0, 1$ con x|I como la subcadena del mensaje I a bob para que él pueda rehacer el mensaje computando $f_c(x'|_{I_c}) \oplus s_c$.

Este protocolo era seguro ante Alicias deshonestas pero no ante Bob deshonestos que podrían aguantar los estados cuánticos hasta que Alice mande las bases que ha usado y así recoger ambos mensajes. La idea del estudio era forzar a Bob a medir antes los estados y luego Alice comprobara una fracción de esta medida antes de enviar las bases. A lo largo de los años se ha seguido investigando la seguridad de este protocolo y cerca de 20 años después Unruh formaliza la equivalencia de BC y OT en el modelo cuántico Universally composable quantum multi-party computation.

Modelos de almacenamiento cuántico limitado

Una de las dificultades a la hora de construir dispositivos cuánticos, tales como ordenadores, es la dificultad de almacenar información cuántica en un sistema físico de forma estable durante mucho tiempo. Construir una memoria cuántica es un logro actualmente inalcanzable, y de lo más buscado en el sector, ya que por ejemplo, Bob, en QKD podría decirle a Alicia que ya los ha medido para que Alicia le mande las bases, y en realidad, si pudiese almacenar los bits cuánticos (fotones), como bits normales, usaría las bases de Alicia para medir (polarizar).

Se podría guardar en una fibra óptica, en un sistema biestable cuántico, pero todas esas memorias ni pueden almacenar mucho (son muy limitadas, complejas de construir), y además la vida de los fotones en esa memoria (tiempo de almacenaje de los qubits) sería muy corta.

Los Limited-quantum-storage models entonces, son modelos que precisamente se basan en esa memoria finita para almacenar qubits, y evitan que se pueda engañar o hacer trampas. Estos modelos, son varios los existentes, y calculan un porcentaje de probabilidad de que la otra persona pueda estar haciendo trampas en este sentido y lo usen con mala voluntad.

Estos cálculos de los modelos se hacen en base a las distintas posibles formas teóricas de almacenar esta información actualmente existentes. Algunos modelos son:

- Bounded-quantum-storage
- Noisy-quantum-storage
- Beyond limited quantum storage
- Cryptographic proof techniques

Por ejemplo: Bounded… se basa en que Alicia antes de enviar Alicia a Bob su base, espere un segundo, que en cuántica eso es muchísimo, y estas memorias no tienen una vida superior a eso.

Computación cuántica delegada

Los ordenadores cuánticos tienen una gran potencia computacional inalcanzable por los ordenadores de hoy día, pero la realidad del sector nos dice que solo estarán disponibles en pocas localizaciones, por lo que se contempla un escenario donde los clientes hagan consultas mediante una red. Surgen dudas sobre la seguridad de la información de los clientes.
El primer caso práctico para delegación de computación cuántica se llamó universal blind quantum computation uBQC de la mano de Broadbent, Fitzsimons y Kashef. En este protocolo el cliente solo necesita poder preparar estados auxiliares de qubits aleatorios sin necesidad de memoria ni procesador cuántico y él será el encargado vía interacción clásica de controlar la computación cuántica deseada. El cliente es el único en saber la salida.
Este protocolo ha sido demostrado experimentalmente y se basa en la codificación conjugada. Por primera vez se utiliza la codificación conjugada para alcanzar tareas computacionales criptográficas.
Esta relación con el código conjugado es más clara en el protocolo quantum computing on encrypted data, QCED. En este protocolo la computación es pública pero ejecutada remotamente en una versión encriptada.fully homomorphic encryption

Coin Flipping

Bob elige aleatoriamente la opción A o B, donde cada una es un tipo de polarización, lo cual Bob desconoce. Ahora Bob comienza a polarizar como de costumbre, a medir todo aleatoriamente como en QKD, y Bob apuesta por una de las dos tipos de polarización. Si Bob pierde, le pedirá a Alicia el set de datos original, y verificará que al polarizar correctamente su resultado es erróneo en los sitios en los que ha usado la polarización opuesta.

Limitaciones y retos

Imposibilidad del compromiso de bits cuánticos