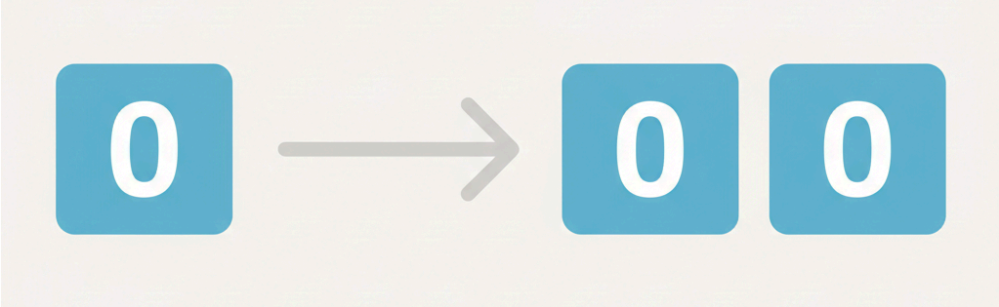
Limitaciones de la Información Cuántica

El Teorema de No-Clonación

La Operación Más Común que Jamás Has Cuestionado

En el mundo de la computación clásica, hay una operación tan fundamental que la damos por sentada, una acción que realizamos miles de veces al día sin pensar.

La Operación "Copiar y Pegar" (Ctrl+C / Ctrl+V)



Tomamos una pieza de información (un bit, un archivo, un texto) y creamos una **copia idéntica e independiente** en otra ubicación de la memoria.
Es la base de la replicación de datos, la comunicación y la corrección de errores clásica.

La Pregunta Cuántica

Ahora, llevemos esta idea a nuestro nuevo mundo.

La Pregunta: ¿Podemos hacer lo mismo con la información cuántica? ¿Podemos tomar un qubit en un estado arbitrario y desconocido $|\psi\rangle$ y crear una copia perfecta en otro qubit?

Intuitivamente, podríamos imaginar una "Compuerta de Clonación" que tome un qubit $|\psi\rangle$ y un qubit "en blanco" $|0\rangle$ y produzca dos copias de $|\psi\rangle$.

$$\text{¿Existe una operación unitaria } \hat{U} \text{ tal que } \hat{U}(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle \text{ ?}$$

La Sorprendente Respuesta de la Naturaleza

La respuesta a esta pregunta es una de las diferencias más profundas y fundamentales entre el mundo clásico y el cuántico.

¡NO!

> **El Teorema de No-Clonación** establece que es **físicamente imposible** crear una copia idéntica e independiente de un estado cuántico **arbitrario y desconocido**.

Este **"no"** no es una limitación tecnológica que superaremos con mejores ordenadores cuánticos. Es una **ley fundamental de la física**, una consecuencia directa de los postulados de la mecánica cuántica.

¿Por Qué es Tan Importante Este "NO"?

El Teorema de No-Clonación no es una simple curiosidad. Tiene implicaciones enormes y de gran alcance:

1. **Seguridad en la Comunicación:** Es la base de la **criptografía cuántica**. Un espía no puede "copiar" un qubit para medirlo sin alterar el original, haciendo que su presencia sea detectable.
2. **Corrección de Errores:** Limita drásticamente cómo podemos corregir errores. No podemos simplemente "hacer una copia de seguridad" de nuestros qubits.
3. **Transferencia de Información:** Para mover un estado cuántico de un lugar a otro, no podemos "copiarlo". Debemos "teleportarlo", un proceso que destruye el estado original (tema que veremos más adelante).
4. **Entendimiento Fundamental:** Nos obliga a pensar en la información cuántica no como un "dato" pasivo, sino como un estado físico delicado y activo.

> En las siguientes diapositivas, vamos a demostrar **por qué** este teorema es cierto, usando las herramientas que ya dominamos: la unitariedad y la linealidad.

La Objeción Más Común

Recordermos que buscamos una compuerta (un operador) que tome un qubit fuente y un qubit destino "en blanco" $|0\rangle$ y que produzca como salida dos copias del qubit fuente.

Al escuchar el Teorema de No-Clonación, una pregunta surge casi de inmediato:

> "¿la compuerta CNOT no hace exactamente eso? Si el objetivo es $|0\rangle$, ¿no 'copia' el estado del control en el objetivo?"

Esta es una objeción excelente y analizarla nos revelará la verdadera naturaleza de la CNOT y del entrelazamiento.

Una Aclaración Fundamental: Copiando Estados Conocidos

Ejemplo: La CNOT como "Copiadora"

La compuerta CNOT parece una copiadora:

- $CNOT_{1,0}(|0\rangle|0\rangle) = |0\rangle|0\rangle$
- $CNOT_{1,0}(|1\rangle|0\rangle) = |1\rangle|1\rangle$

Si sabemos que el primer qubit (el qubit $|\psi\rangle$ que queremos copiar) es $|0\rangle$ o $|1\rangle$, la $CNOT_{1,0}$ efectivamente "copia" ese bit en el segundo qubit.

El teorema **NO** prohíbe copiar estados si sabemos de antemano que pertenecen a una base ortonormal conocida (como la base computacional).

> **El problema no es copiar $|0\rangle$ o $|1\rangle$. El problema es construir una única máquina que pueda copiar cualquier estado de la esfera de Bloch sin saber cuál es de antemano.**

El Comportamiento "Clásico" de la CNOT

La confusión es comprensible, porque si nos limitamos a la **base computacional**, la CNOT se comporta exactamente como una máquina de copiar.

Recordemos su acción (control en q_1, objetivo en q_0):

- Si el estado de entrada es $|0\rangle|0\rangle$:

$$\text{CNOT}|00\rangle = |00\rangle$$

- Si el estado de entrada es $|1\rangle|0\rangle$:

$$\text{CNOT}|10\rangle = |11\rangle$$

Podemos resumir esto como:

$$\text{CNOT}(|x\rangle|0\rangle) = |x\rangle|x\rangle \quad \text{para } x \in \{0, 1\}$$

> Si **sabemos** que el qubit de control es $|0\rangle$ o $|1\rangle$, la CNOT sí copia ese bit clásico. Pero el Teorema de No-Clonación trata sobre un estado **desconocido y arbitrario**.

Revisa la Sección 1 del cuaderno jupyter

clase10-qiskit.ipynb

¿CNOT no puede clonar cualquier estado?

Veamos el análisis algebraico de aplicar $CNOT_{1,0}$ al ket $|+\rangle|0\rangle$

El Problema: $\mathrm{CNOT}(|+\rangle|0\rangle) = |+\rangle|+\rangle$??

El Cálculo (usando la linealidad):

$$\mathrm{CNOT}\Big((\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes |0\rangle\Big) = \mathrm{CNOT}\Big(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\Big)$$

$$= \frac{1}{\sqrt{2}}\Big(\mathrm{CNOT}|00\rangle + \mathrm{CNOT}|10\rangle\Big)$$

$$= \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = |\Phi^+\rangle$$

> El resultado **NO** es dos copias de $|+\rangle$. El resultado es un **estado de Bell máximamente entrelazado**.

La Comparación Final: Clonación vs. Entrelazamiento

Comparemos el resultado que obtuvimos con el que un clonador ideal debería haber producido.

Resultado Real (lo que la CNOT hace):

$$\text{CNOT}(|+\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

(Un estado entrelazado)

Resultado Ideal (lo que un clonador haría):

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

$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

(Un estado separable)

Claramente, los dos resultados son completamente diferentes.

La Verdadera Naturaleza de la CNOT

La CNOT **no es** una "copiadora de estados cuánticos". Su verdadera función es mucho más sutil y poderosa.

> La compuerta CNOT **no clona el estado**, sino que **crea y propaga correlaciones** entre los qubits.

Analicemos sus dos modos de operación fundamentales:

- **Si el control está en un estado base ($|0\rangle$ o $|1\rangle$):** La CNOT actúa como una compuerta clásica condicional. **No puede crear entrelazamiento.** Un estado de entrada separable siempre resultará en un estado de salida separable.
- **Si el control está en una superposición:** La CNOT explota el paralelismo cuántico. "Extiende" la superposición del control al objetivo, transformando un estado separable en un **estado entrelazado**.

> En resumen: **la CNOT no clona, entrelaza**. Es nuestra herramienta fundamental para generar el recurso más valioso de la computación cuántica, y solo puede hacerlo cuando el qubit de control está en superposición.

La Declaración Formal del Teorema de No-Clonación

El Teorema de No-Clonación es una afirmación precisa con condiciones muy específicas.

> **Teorema:** Es imposible construir un operador unitario universal $\hat{U}$ que pueda crear una copia **idéntica** e **independiente** de un estado cuántico **desconocido** y arbitrario.

Analicemos cada una de sus partes. Las tres palabras clave —**idéntica, independiente y desconocido**— son las que le dan al teorema su verdadero significado y alcance.

¿Qué Significa Realmente "Clonar"?

1. **"Idéntica"**:
   - La copia debe ser perfecta, de alta fidelidad. No se trata de una aproximación. El estado del segundo qubit debe ser exactamente $|\psi\rangle$.
2. **"Independiente"**:
   - Esta es la condición más sutil. El estado final del sistema de dos qubits debe ser un **estado producto (separable)**, $|\psi\rangle \otimes |\psi\rangle$.
   - Esto asegura que la copia no esté entrelazada con el original. Un estado entrelazado como $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ contiene dos qubits, pero ninguno de ellos tiene un estado individual propio. No son copias independientes.
3. **"Desconocido"**:
   - Esta es la condición más importante. No sabemos de antemano cuál es el estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. El "clonador" debe ser una máquina universal que funcione para **cualquier** estado que le demos.

La Prueba Formal por Contradicción

Traduciendo la Clonación a Ecuaciones

Ahora, formalicemos la hipótesis que vamos a refutar.

El Objetivo: Queremos una operación que transforme un estado inicial $|\psi\rangle|s\rangle$ en un estado final $|\psi\rangle|\psi\rangle$. Donde $|s\rangle$ es un estado "en blanco" estándar, independiente de $|\psi\rangle$ (usaremos $|s\rangle = |0\rangle$).

El Mecanismo: Según los postulados de la mecánica cuántica, toda evolución debe ser descrita por un **operador unitario** $\hat{U}$.

Traduciendo la Clonación a Ecuaciones

La Hipótesis que refutaremos:

> **"Supongamos que existe un clonador cuántico universal."**
>
> Matemáticamente, esto significa que existe un único operador unitario $\hat{U}$ tal que para **cualquier** estado $|\psi\rangle$:
>
> $$\hat{U}(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
>
> donde $|s\rangle$ es un estado "en blanco" estándar, independiente de $|\psi\rangle$ (usaremos $|s\rangle = |0\rangle$).

En las siguientes diapositivas, demostraremos que esta hipótesis conduce a una **contradicción matemática**.

Paso 1: Asumimos la Existencia del Clonador

Hipótesis: Existe un operador unitario universal $\hat{U}$ que clona cualquier estado.

Mostraremos que esta hipótesis solo funciona bajo condiciones tan restrictivas que la máquina deja de ser "universal".

Estrategia:

1. Elegimos dos estados cuánticos **arbitrarios y distintos**, $|\psi\rangle$ y $|\phi\rangle$.
2. Aplicamos nuestra supuesta máquina clonadora a cada uno de ellos por separado.
3. Analizamos la relación entre los estados clonados resultantes.

Paso 2: Plantear la Estrategia de la Prueba

Tenemos dos ecuaciones que describen la acción de nuestro clonador:

Ecuación A: $\hat{U}(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$

Ecuación B: $\hat{U}(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$

Nuestra estrategia será la siguiente:

1. Calcularemos el producto interno entre el **lado izquierdo** de la Ecuación A (tomado como bra) y el **lado izquierdo** de la Ecuación B (tomado como ket). Es decir:

$$\langle \hat{U}(|\psi\rangle \otimes |0\rangle) \,|\, \hat{U}(|\phi\rangle \otimes |0\rangle) \rangle$$

2. Luego, calcularemos el producto interno entre el **lado derecho** de la Ecuación A (bra) y el **lado derecho** de la Ecuación B (ket). Es decir:

$$\langle |\psi\rangle \otimes |\psi\rangle \,|\, |\phi\rangle \otimes |\phi\rangle \rangle$$

3. Como los lados izquierdos son iguales a los derechos, los resultados de ambos cálculos **deben ser idénticos**.

Paso 3: Calcular el Producto Interno de los Lados Izquierdos

Calculamos la expresión del bra:

$$\langle \hat{U}(|\psi\rangle \otimes |0\rangle) \, | = \left(\hat{U}(|\psi\rangle \otimes |0\rangle)\right)^\dagger$$

Usando la regla $(A \cdot B)^\dagger = B^\dagger \cdot A^\dagger$:

$$= (|\psi\rangle \otimes |0\rangle)^\dagger \cdot \hat{U}^\dagger$$

Y usando la regla $(C \otimes D)^\dagger = C^\dagger \otimes D^\dagger$:

$$= (\langle\psi| \otimes \langle 0|) \cdot \hat{U}^\dagger$$

Multiplicando el Bra por el Ket $\hat{U}(|\phi\rangle \otimes |0\rangle)$ para obtener el producto interior que buscamos

$$\left((\langle\psi| \otimes \langle 0|)\hat{U}^\dagger\right)\left(\hat{U}(|\phi\rangle \otimes |0\rangle)\right)$$

Reagrupamos los operadores $\hat{U}$:

$$(\langle\psi| \otimes \langle 0|)(\hat{U}^\dagger \hat{U})(|\phi\rangle \otimes |0\rangle)$$

Como $\hat{U}$ es unitario, $\hat{U}^\dagger \hat{U} = \hat{I}$. La expresión se simplifica:

$$(\langle\psi| \otimes \langle 0|) \cdot (|\phi\rangle \otimes |0\rangle)$$

Usamos la regla $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$:

$$(\langle\psi|\phi\rangle) \otimes (\langle 0|0\rangle)$$

Como el resultado de cada producto interno es un escalar, el producto tensorial se convierte en una multiplicación normal:

$$= (\langle\psi|\phi\rangle) \cdot (1) = \langle\psi|\phi\rangle$$

> **Resultado 1:** El producto interno de los lados izquierdos de las **ecuaciones A y B** es $\langle\psi|\phi\rangle$.

Paso 4: Calcular el Producto Interno de los Lados Derechos

Ahora, calculamos el producto interno entre las expresiones del lado derecho de nuestras ecuaciones. El producto interno que buscamos es:

$$\langle |\psi\rangle \otimes |\psi\rangle \,|\, |\phi\rangle \otimes |\phi\rangle \rangle$$

Ket del lado derecho de B:

$$|\phi\rangle \otimes |\phi\rangle$$

Bra del lado derecho de A:

$$\langle |\psi\rangle \otimes |\psi\rangle \,| = \Big(|\psi\rangle \otimes |\psi\rangle\Big)^\dagger$$

Usando la regla $(C \otimes D)^\dagger = C^\dagger \otimes D^\dagger$:

$$= \langle\psi| \otimes \langle\psi|$$

Multiplicando el Bra por el Ket para obtener el producto interior:

$$\Big(\langle\psi| \otimes \langle\psi|\Big) \cdot \Big(|\phi\rangle \otimes |\phi\rangle\Big)$$

Usamos la regla de multiplicación de productos tensoriales $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$:

$$(\langle\psi|\phi\rangle) \otimes (\langle\psi|\phi\rangle)$$

Como el resultado de cada producto interno es el mismo escalar $\langle\psi|\phi\rangle$, el producto tensorial se convierte en una multiplicación normal:

$$= (\langle\psi|\phi\rangle) \cdot (\langle\psi|\phi\rangle) = (\langle\psi|\phi\rangle)^2$$

> **Resultado 2:** El producto interno de los lados derechos de las **ecuaciones A y B** es $(\langle\psi|\phi\rangle)^2$.

La Igualdad Crucial

Ahora que hemos calculado ambos productos internos, los igualamos.

Resultado 1 (de los lados izquierdos): $\langle\psi|\phi\rangle$

Resultado 2 (de los lados derechos): $(\langle\psi|\phi\rangle)^2$

Como los lados de las ecuaciones A y B son iguales, sus productos internos también deben serlo. Por lo tanto:

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$$

> Esta es la ecuación que debe cumplir nuestra supuesta máquina clonadora para dos estados cualquiera. En la siguiente diapositiva, veremos por qué esto conduce a una contradicción.

Paso 5: El Momento de la Contradicción

Hemos llegado a una ecuación sorprendentemente simple que debe ser cierta para **cualesquiera** dos estados $|\psi\rangle$ y $|\phi\rangle$.

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$$

Esto implica:

$$(\langle\psi|\phi\rangle)^2 - \langle\psi|\phi\rangle = 0$$

$$\langle\psi|\phi\rangle(1 - \langle\psi|\phi\rangle) = 0$$

Por lo tanto, $\langle\psi|\phi\rangle = 0$ o 1.

La Conclusión Inevitable:

Nuestra supuesta máquina de clonación universal solo funciona si el producto interno $\langle\psi|\phi\rangle$ entre los dos estados que intentamos clonar es **0** o **1**.

Análisis: ¿Qué Significa que $\langle\psi|\phi\rangle$ sea 0 o 1?

Si $\langle\psi|\phi\rangle = 1$:
Esto solo ocurre si los estados son idénticos (salvo una fase global). Básicamente, $|\psi\rangle = |\phi\rangle$.

Si $\langle\psi|\phi\rangle = 0$:
Esto significa que los estados son **ortogonales** (perfectamente distinguibles), como $|0\rangle$ y $|1\rangle$.

La Contradicción:
El clonador solo funciona para estados que ya son idénticos o que son ortogonales. Pero, ¿qué pasa si le damos un estado no ortogonal, como $|\psi\rangle = |0\rangle$ y $|\phi\rangle = |+\rangle$?

$$\langle 0|+\rangle = \frac{1}{\sqrt{2}}$$

Nuestra ecuación requeriría que $\frac{1}{\sqrt{2}} = (\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$, lo cual es **falso**.

> **Conclusión Final:** La hipótesis de un clonador "universal" es falsa. Una máquina de este tipo no puede existir porque viola los principios de la mecánica cuántica (la linealidad de la unitariedad) para la gran mayoría de los estados posibles.

Qué significa esta conclusión

> “No puede existir un operador unitario que clone estados no ortogonales” significa que **no existe un único operador unitario** $\hat{U}$ que sea capaz de clonar dos o más estados distintos que **no sean ortogonales entre sí**.

Sin embargo, nada impide que exista una operador U_ψ que clone **un estado en particular** $|\psi\rangle$.

De hecho, siempre podemos construir un operador que actúe así:

$$\hat{U}_\psi|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

El truco es que esa $\hat{U}_\psi$ depende del propio $|\psi\rangle$.
No es **universal**: sólo funciona para ese estado específico (o para los ortogonales a él, como veremos).

La Causa Raíz del Problema: La Linealidad

Una Segunda Prueba: Atacando el Problema con la Linealidad

La prueba anterior usó la propiedad de la **unitariedad**. Ahora, usaremos la otra propiedad fundamental de toda evolución cuántica: la **linealidad**.

Este enfoque es quizás más intuitivo y revela que la propia estructura de la superposición es lo que impide la clonación.

La Estrategia:
Vamos a analizar qué le sucede a un **estado de superposición** si lo pasamos por nuestra hipotética máquina clonadora, siguiendo dos caminos:

- **Camino 1:** Lo que la máquina **debería** hacer (clonar la superposición completa).
- **Camino 2:** Lo que la máquina **está obligada** a hacer por el postulado de la linealidad.

Si los dos caminos llevan a resultados diferentes, nuestra máquina es imposible.

El Estado de Prueba

Tomemos como ejemplo un estado general en superposición, $|\chi\rangle$, construido a partir de dos estados base ortonormales, $|0\rangle$ y $|1\rangle$:

$$|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$$

(Un ejemplo concreto podría ser el estado $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$).

Nuestra Hipótesis Clonadora:

Recordemos que nuestra máquina $\hat{U}$ supuestamente puede clonar *cualquier* estado, incluyendo $|0\rangle$, $|1\rangle$ y, fundamentalmente, $|\chi\rangle$.

- $\hat{U}(|0\rangle|0\rangle) = |0\rangle|0\rangle$
- $\hat{U}(|1\rangle|0\rangle) = |1\rangle|1\rangle$
- $\hat{U}(|\chi\rangle|0\rangle) = |\chi\rangle|\chi\rangle$

Ahora, sigamos los dos caminos.

Camino 1: El Resultado Ideal (Lo que "Debería" Pasar)

Si nuestra máquina es un clonador perfecto, debe tomar el estado $|\chi\rangle|0\rangle$ y producir el estado $|\chi\rangle|\chi\rangle$. Vamos a expandir esta expresión:

$$|\chi\rangle \otimes |\chi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

Distribuyendo el producto tensorial:

$$= \alpha^2(|0\rangle|0\rangle) + \alpha\beta(|0\rangle|1\rangle) + \beta\alpha(|1\rangle|0\rangle) + \beta^2(|1\rangle|1\rangle)$$

Este es el estado **separable** que un clonador ideal debería producir.

Camino 2: La Realidad de la Linealidad (Lo que "Debe" Pasar)

Ahora, calculemos el resultado aplicando la **linealidad**, que es una regla inquebrantable de la mecánica cuántica.

Partimos de la entrada $\hat{U}(|\chi\rangle|0\rangle)$ y sustituimos la definición de $|\chi\rangle$:

$$\hat{U}\Big((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle\Big) = \hat{U}\Big(\alpha(|0\rangle|0\rangle) + \beta(|1\rangle|0\rangle)\Big)$$

Por la linealidad de $\hat{U}$, podemos distribuir el operador:

$$= \alpha\Big(\hat{U}(|0\rangle|0\rangle)\Big) + \beta\Big(\hat{U}(|1\rangle|0\rangle)\Big)$$

Ahora usamos nuestra hipótesis de que la máquina clona los estados base correctamente:

$$= \alpha(|0\rangle|0\rangle) + \beta(|1\rangle|1\rangle)$$

> El resultado es el famoso estado de Bell (si $\alpha = \beta = 1/\sqrt{2}$), un estado **máximamente entrelazado**.

La Contradicción es Evidente

Ahora, comparemos los resultados de los dos caminos.

Camino 1 (Resultado Ideal):

$$\alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle$$

(Un estado separable con 4 términos)

Camino 2 (Resultado por Linealidad):

$$\alpha|00\rangle + \beta|11\rangle$$

(Un estado entrelazado con solo 2 términos)

Salvo casos triviales (donde $\alpha = 0$ o $\beta = 0$), estos dos estados son **fundamentalmente diferentes**.

> **Conclusión:** La linealidad, un pilar de la mecánica cuántica, nos obliga a seguir el Camino 2. El resultado ideal del Camino 1 es incompatible con este principio. Por lo tanto, una máquina que siga el Camino 1 **no puede existir**.

Resumen: La Linealidad Prohíbe Clonar

- La **linealidad** aplicada a una tarea de clonación, produce un **estado entrelazado**, no dos copias independientes.
- La misma propiedad que nos da el poder de la superposición y la interferencia (la linealidad) es la que impone esta restricción fundamental. No podemos tener una cosa sin la otra.

Medición en Diferentes Bases

La Pregunta Práctica: ¿Cómo Medimos en la Base X?

Hasta ahora, todas nuestras mediciones han sido en la **base computacional** $\{|0\rangle, |1\rangle\}$. Esto corresponde a "preguntarle" al qubit: "¿Eres un 0 o un 1?".

Matemáticamente, esta es una medición con respecto al **observable Z**, cuyos autovectores son $|0\rangle$ y $|1\rangle$.

Pero, ¿qué pasa si queremos medir con respecto al **observable X**?

- Sus autovectores son $|+\rangle$ y $|-\rangle$.
- Esto equivale a preguntarle al qubit: "¿Eres un $|+\rangle$ o un $|-\rangle$?"

El Problema: El hardware cuántico y los simuladores (como Qiskit) **solo saben cómo realizar mediciones en la base Z**. No existen "compuertas de medición en X" nativas.

La Solución: Un "Truco" con Cambio de Base

La solución es elegante y se basa en la reversibilidad de las operaciones unitarias.

> **La Receta:** Para medir en una base diferente (ej: la base X), primero aplicamos una transformación unitaria que **rota** esa base de interés a la base computacional. Luego, realizamos una medición estándar en Z.

El Principio:

- Si el estado original *era* $|+\rangle$, la rotación (con la compuerta H) lo convertirá en el estado $|0\rangle$.
- Ahora, al realizar una medición en la base Z, el estado colapsará al autovector $|0\rangle$ con 100% de probabilidad.
- El ordenador cuántico nos reportará el **resultado clásico '0'**.
- Al ver el resultado `'0'`, nosotros **inferimos** que el estado original, antes de la rotación, era $|+\rangle$.

La Estrategia: "Deshacer" el Cambio de Base

Para medir en una base $\{|v_0\rangle, |v_1\rangle\}$, necesitamos aplicar el operador que la transforma de vuelta a la base computacional $\{|0\rangle, |1\rangle\}$.

Convención de Nomenclatura:

1. Llamamos $\hat{U}$ a la transformación "hacia adelante", la que **crea** la nueva base a partir de la computacional:

$$\hat{U}|0\rangle = |v_0\rangle \quad , \quad \hat{U}|1\rangle = |v_1\rangle$$

2. La operación que necesitamos para preparar la medición es la **inversa**, que "deshace" esta creación:

$$\hat{U}^\dagger|v_0\rangle = |0\rangle \quad , \quad \hat{U}^\dagger|v_1\rangle = |1\rangle$$

> **Principio de Medición:** Para medir en una nueva base, aplicamos el operador $\hat{U}^\dagger$ (el inverso del que crea la base) y luego realizamos una medición estándar en Z.

Medición en la Base X (Hadamard)

1. La Base de Interés (Base X): $\{|+\rangle, |-\rangle\}$

2. El Operador de Creación ($\hat{U}$):
El operador que crea la base X a partir de la base computacional es la **compuerta Hadamard**:

$$H|0\rangle = |+\rangle \quad , \quad H|1\rangle = |-\rangle$$

Por lo tanto, para la base X, nuestro operador de cambio de base es $\hat{U} = H$.

3. El Operador de Medición ($\hat{U}^\dagger$):
Para medir, necesitamos el operador inverso, $\hat{U}^\dagger = H^\dagger$.
Recordemos que la Hadamard es una compuerta **Hermitiana**, lo que significa que es su propia adjunta:

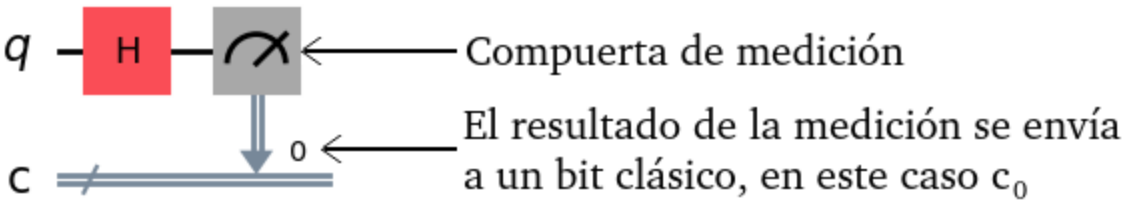
$$H^\dagger = H$$

Esto nos lleva a una conclusión muy conveniente: la misma compuerta H que *crea* la base de Hadamard es también la que la *deshace* para la medición.

$$H|+\rangle = |0\rangle \quad , \quad H|-\rangle = |1\rangle$$

3. El Circuito:

El circuito para medir en la base X es:



Interpretación del Resultado Clásico:

Si medimos `'0'`, el estado **antes** de la H era $|+\rangle$.

Si medimos `'1'`, el estado **antes** de la H era $|-\rangle$.

Medición en la Base Y (Circular)

1. La Base de Interés (Base Y): $\{|i\rangle, |-i\rangle\}$

2. El Operador de Creación ($\hat{U}$):
El operador que crea la base Y a partir de la base computacional es $\hat{U} = S \cdot H$.

$$(S \cdot H)|0\rangle = |i\rangle \quad , \quad (S \cdot H)|1\rangle = |-i\rangle$$

(Nota: El circuito se construye en orden inverso: primero H, luego S).

3. El Operador de Medición ($\hat{U}^\dagger$):
Para medir, necesitamos el inverso, $\hat{U}^\dagger$. Usando la regla $(A \cdot B)^\dagger = B^\dagger \cdot A^\dagger$:

$$\hat{U}^\dagger = (S \cdot H)^\dagger = H^\dagger \cdot S^\dagger$$

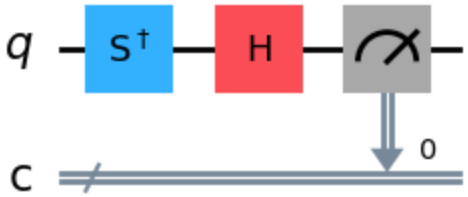
Como H es Hermitiana ($H^\dagger = H$), la expresión final es: $\hat{U}^\dagger = H \cdot S^\dagger$

Este es el operador que "deshace" la base Y, devolviéndola a la base computacional para la medición.

$$(H \cdot S^\dagger)|i\rangle = |0\rangle \quad , \quad (H \cdot S^\dagger)|-i\rangle = |1\rangle$$

(Nota: El circuito para este operador se construye aplicando primero $S^\dagger$ y luego H).

3. El Circuito:



Interpretación del Resultado Clásico:

Si medimos `'0'`, el estado original era $|i\rangle$.

Si medimos `'1'`, el estado original era $|-i\rangle$.

Resumen: La Estrategia Universal

La medición en bases no computacionales es un pilar de muchos algoritmos y protocolos.

El Principio General:

Medir en una base ortonormal $\{|v_0\rangle, |v_1\rangle\}$ es equivalente a:

1. Encontrar el operador unitario $\hat{U}^\dagger$ que realiza el cambio de base: $\hat{U}^\dagger|v_0\rangle = |0\rangle$ y $\hat{U}^\dagger|v_1\rangle = |1\rangle$.
2. Aplicar dicho operador $\hat{U}^\dagger$ al estado del qubit.
3. Realizar una medición estándar en la base Z.

Ahora que dominamos esta técnica, tenemos todas las herramientas necesarias para entender el protocolo de criptografía cuántica **BB84**.

Revisa la Sección 2 del cuaderno jupyter

clase10-qiskit.ipynb

Criptografía Cuántica

El Protocolo BB84

La Búsqueda de la Seguridad Perfecta

La mayoría de los sistemas criptográficos que usamos hoy en día, desde RSA hasta la criptografía postcuántica, basan su seguridad en un principio: **la dificultad computacional**.

Confían en problemas matemáticos que *creemos* que son demasiado difíciles de resolver para los ordenadores actuales (y futuros). Pero esta es una **seguridad condicional**: no tenemos una prueba matemática de que sean irrompibles para siempre.

Esto nos lleva a una pregunta fundamental:

> **¿Cómo sería un sistema de cifrado teóricamente "perfecto"?** Uno cuya seguridad no dependa de suposiciones, sino que sea **incondicionalmente seguro** y **absolutamente irrompible**.
>
> **¿Podría existir un sistema de estas características?**

La Respuesta: El Cifrado de Vernam (One-Time Pad)

El sistema criptográfico perfecto existe desde 1917 y es sorprendentemente simple. Se conoce como el **cifrado de Vernam** o **One-Time Pad (OTP)**.

La Receta Perfecta:

- **Clave Aleatoria:** Alice y Bob comparten una clave secreta que es **totalmente aleatoria**.
- **Clave Larga:** La clave debe ser **tan larga como el mensaje** que se quiere enviar.
- **Clave de un Solo Uso:** La clave **nunca se reutiliza**.

El Mecanismo (XOR):

- **Cifrado (Alice):** `Mensaje Cifrado = Mensaje XOR Clave`
- **Descifrado (Bob):** `Mensaje = Mensaje Cifrado XOR Clave`

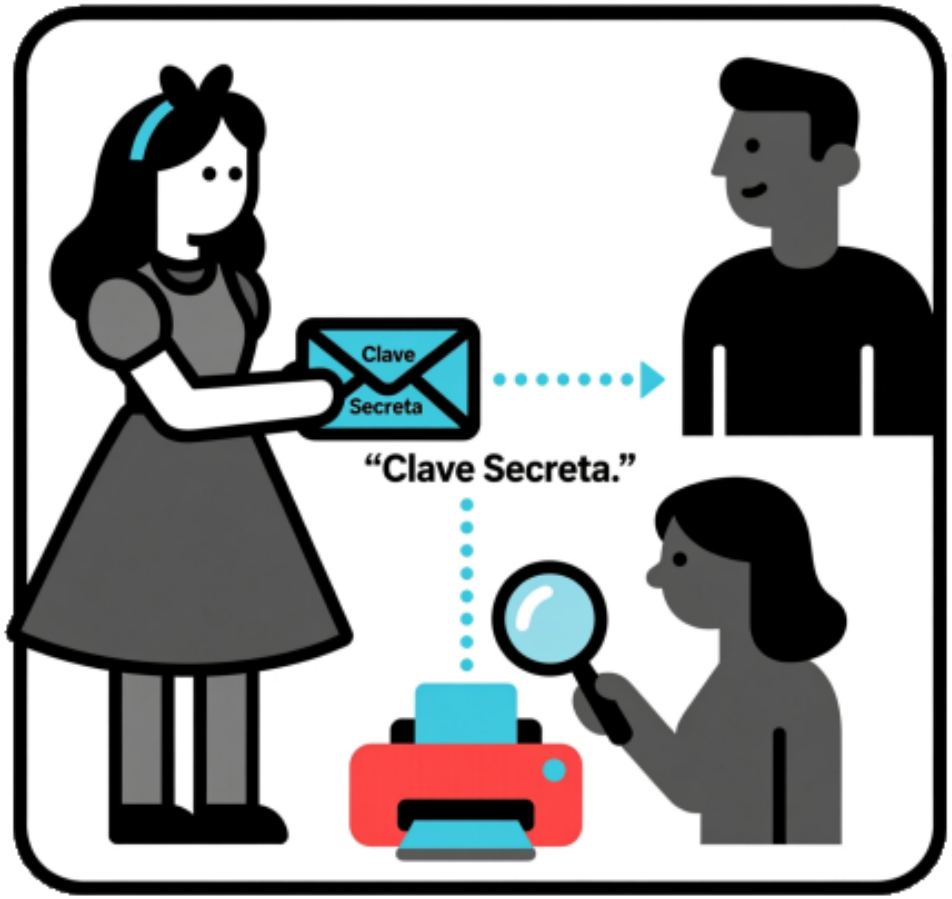
> Se ha demostrado matemáticamente que este sistema es **incondicionalmente seguro**. Un espía que intercepte el mensaje cifrado no obtiene absolutamente ninguna información sobre el mensaje original, ya que cualquier mensaje es igualmente probable.

El Talón de Aquiles: La Distribución de la Clave

El sistema es perfecto, pero tiene un problema fundamental:

> **¿Cómo pueden Alice y Bob obtener esa clave secreta compartida de forma segura, especialmente si nunca se han encontrado físicamente?**

Si Alice envía la clave a Bob por un canal clásico (internet, teléfono, radio...), una tercera persona, la espía **Eva**, puede estar escuchando.



Eva puede simplemente **leer la clave y copiarla** mientras viaja. Alice y Bob nunca sabrán que su "secreto" ha sido comprometido. Este es el **problema de la distribución de claves**.

El Objetivo del Protocolo BB84

El protocolo BB84, propuesto por Charles Bennett y Gilles Brassard en 1984, no es un método para enviar mensajes cifrados sino para obtener de manera segura una clave compartida.

> **El objetivo de BB84 es permitir que Alice y Bob creen una clave secreta compartida a partir de cero, con un alto grado de confianza de que nadie más la conoce.**

La genialidad del protocolo es que utiliza los principios de la mecánica cuántica para **revelar la presencia de cualquier espía**.

El Alfabeto Cuántico de Alice

Para enviar su clave secreta, Alice utilizará un "alfabeto" cuántico. Su estrategia se basa en dos elecciones aleatorias para cada bit que quiere enviar:

1. **El Bit Clásico:** El valor que quiere comunicar ('0' o '1').
2. **La Base de Codificación:** Una elección al azar entre la **Base Z** (nuestra base computacional) y la **Base X** (la base de Hadamard).

Esto da lugar a cuatro posibles estados para enviar, según la siguiente tabla de codificación:

Bit a Enviar	Base Elegida	Qubit Enviado
0	**Z**	$\|0\rangle$
1	**Z**	$\|1\rangle$
0	**X**	$\|+\rangle$
1	**X**	$\|-\rangle$

> **La Clave de la Seguridad:** Un bit '0' puede ser enviado como $|0\rangle$ o como $|+\rangle$. Estos dos estados **no son ortogonales** ($\langle 0|+\rangle = 1/\sqrt{2}$). Como veremos, esto hace imposible que un espía los distinga con certeza sin conocer la base.

La Fase de Envío y Recepción

El protocolo comienza con el intercambio de qubits. Ni Bob ni Eva conocen las bases que Alice ha elegido.

1. **Alice** genera su cadena de bits y su cadena de bases. Prepara y envía los qubits uno por uno.
2. **Bob**, por cada qubit que recibe, elige su propia base de medición de forma aleatoria (Z o X) y anota el resultado.

Ejemplo de un Intercambio (sin espía):

Paso	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Bit de Alice	0	1	1	0	1	0	0	1
Base de Alice	Z	Z	X	Z	X	X	Z	X
Qubit Enviado	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$
---	---	---	---	---	---	---	---	---
Base de Bob	Z	X	X	Z	Z	X	X	X
Resultado de Bob	0	1	1	0	1	0	1	1

Analizando el Resultado (Sin Espía)

Observemos la tabla del intercambio. Ocurren dos situaciones:

1. Las Bases Coinciden (Resaltado en verde):

- En los pasos 1, 3, 4, 6 y 8, Bob eligió por casualidad la misma base que Alice.
- **En cada uno de estos casos, el bit que Bob midió es idéntico al que Alice envió.** (¡La medición funciona!)

2. Las Bases NO Coinciden (Resaltado en rojo):

- En los pasos 2, 5 y 7, el resultado de Bob es **aleatorio** y no guarda correlación con el bit de Alice. Estos bits son inútiles y se descartarán.

Paso	1	2	3	4	5	6	7	8
Bit de Alice	0	1	1	0	1	0	0	1
Base de Alice	Z	Z	X	Z	X	X	Z	X
Base de Bob	Z	X	X	Z	Z	X	X	X
Resultado de Bob	0	1	1	0	1	0	1	1

Conclusión Parcial: Los bits donde las bases coinciden son potencialmente útiles. El siguiente paso es descubrir cuáles son cuáles sin revelar los valores de los bits.

El Dilema: ¿Cómo Separar el Trigo de la Paja?

- Alice tiene su cadena de bits original. Bob tiene una nueva cadena de bits.
- Algunos de los bits de Bob son **correctos** (donde las bases coincidieron).
- Otros son **aleatorios e inútiles** (donde las bases no coincidieron).

El Problema Fundamental:

> En este momento, **ninguno de los dos sabe qué bits son los correctos**. ¿Cómo pueden "sincronizar" sus listas y descartar los bits inútiles?

Acto 3. La Solución: Una Conversación Pública

Para resolver su dilema, Alice y Bob recurren a un canal de comunicación clásico (público), como un teléfono o internet.

El Paso Crucial: La Reconciliación de Bases

- Alice y Bob **anuncian públicamente** la secuencia de **bases** que usaron para cada qubit.
- **Importante:** ¡No revelan los bits que enviaron o midieron, solo las bases! Esta información, por sí sola, es inútil para Eva.

Ejemplo:

Paso	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Base de Alice	Z	Z	X	Z	X	X	Z	X
Base de Bob	Z	X	X	Z	Z	X	X	X
¿Coinciden?	**Sí**	**No**	**Sí**	**Sí**	**No**	**Sí**	**No**	**Sí**

Ahora ambos saben qué mediciones son válidas (las verdes) y cuáles deben descartar (las rojas).

La "Clave en Crudo"

Después de descartar los resultados de las bases no coincidentes, Alice y Bob se quedan con una cadena de bits más corta, que *debería* ser idéntica.

Ejemplo (Continuación):

- Se quedan con los bits de los pasos 1, 3, 4, 6 y 8.

Bit Original de Alice:
`0` `1` `0` `0` `1`

Resultado de Bob (en bases coincidentes):
`0` `1` `0` `0` `1`

> ¡Éxito! Ahora ambos comparten la misma clave secreta: **01001**.
>
> Pero... ¿están **seguros** de que están solos? ¿Y si Eva estuvo escuchando en el canal cuántico?

La Confrontación: ¿Qué Pasa si Eva Espía?

Ahora introducimos a la espía, **Eva**. Ella intercepta los qubits que Alice envía a Bob.

El Dilema de Eva:

1. Para obtener información, Eva **debe medir** cada qubit.
2. Ella **no sabe** en qué base lo envió Alice (Z o X). Debe adivinar.
3. El **Teorema de No-Clonación** le prohíbe hacer una copia perfecta para medirla después. Debe medir el original y luego intentar reenviar algo a Bob para no ser detectada.

> La intervención de Eva es un proceso de **Interceptar-Medir-Reenviar**. Este proceso, como veremos, inevitablemente deja una huella.

El Acto del Crimen y la Evidencia

La presencia de Eva se detecta cuando ella elige una base de medición diferente a la que Alice y Bob han elegido y verificado su coincidencia. Su medición perturba el estado y crea un error detectable.

La Anatomía de un Error Detectado:

Actor	Acción	Estado del Qubit	Resultado Clásico
Alice	Envía '0' en Base X	$\|+\rangle$	Alice sabe: `'0'`
Eva	Mide en Base Z (error)	Colapsa a $\|0\rangle$	Eva obtiene: `'0'`
Eva	Reenvía el estado colapsado	$\|0\rangle$	
Bob	Mide en Base X (acierto)	Colapsa a $\|-\rangle$	Bob obtiene: **`'1'`**

(Nota: En el último paso, la medición de Bob del estado $|0\rangle$ en la base X da '0' o '1' con 50% de probabilidad. Hemos mostrado el caso en el que el resultado es diferente para resaltar el error).

La Evidencia:

> Alice y Bob, al comparar públicamente sus bases, descubren que para este qubit ambos usaron la Base X. Deberían haber obtenido el mismo bit. Sin embargo, Alice tiene un '0' y Bob tiene un '1'. **Esta discrepancia es la prueba irrefutable de la presencia de Eva.**

La Verificación Final

El Paso de Verificación:

- Alice y Bob eligen un **subconjunto aleatorio** de su "clave en crudo" (por ejemplo, la mitad de los bits).
- **Anuncian públicamente** los valores de los bits de **solo ese subconjunto**.
- Comparan bit a bit.

Los Dos Posibles Veredictos:

1. **Sin Errores:** Si todos los bits de prueba coinciden, asumen con alta confianza que no hubo espionaje. Descartan los bits de prueba (que ya no son secretos) y se quedan con el resto como su **clave final segura**.
2. **Con Errores:** Si encuentran discrepancias, saben que Eva estuvo allí. La tasa de error (QBER) les indica cuánto escuchó. Si el error es significativo, **descartan la clave por completo** y vuelven a empezar.

> **Eva no puede obtener información sin introducir errores.** Su intento de espionaje queda inevitablemente expuesto.

Los Pasos Finales (Procesamiento Clásico)

Incluso sin espía, la clave aún puede no ser perfecta por causa del ruido (**QBER baja**). Se deben realizar dos pasos finales a través del canal público para obtener una clave útil:

- **Reconciliación de Errores:** Usan un protocolo (como *Cascade*) para encontrar y corregir las discrepancias en sus claves, asegurando que sean **100% idénticas**. Este proceso revela algo de información.
- **Amplificación de Privacidad:** Aplican una función hash para "comprimir" su clave a una más corta, eliminando cualquier información parcial que un espía (o el ruido) pudiera haber filtrado.

> **Resultado:** Obtienen una **clave final más corta**, pero que es **perfectamente idéntica y segura**.

¿Por Qué es Seguro? La Física como Escudo

La seguridad del protocolo BB84 no se basa en suposiciones sobre la capacidad computacional de un espía (como en la criptografía clásica). Se basa en dos pilares inquebrantables de la física cuántica:

1. **Colapso de la Medición:**

   > El acto de medir un estado cuántico puede alterarlo. Si Eva mide en la base equivocada, "daña" el qubit, introduciendo errores detectables.

2. **Teorema de No-Clonación:**

   > Eva no puede evitar el problema anterior haciendo una copia del qubit para medirla tranquilamente. La clonación de un estado desconocido es imposible.

> **Cualquier intento de obtener información sobre la clave deja una huella. La física misma actúa como el sistema de alarma.**

El Rol Práctico de BB84: Un Sistema Híbrido

Una pregunta clave es: ¿Usamos la clave generada por BB84 para un One-Time Pad?

Generalmente, no. El protocolo produce una clave final mucho más corta que la comunicación original. Sería ineficiente para cifrar mensajes largos.

En la práctica, BB84 se utiliza como un **Sistema de Distribución de Claves Cuánticas (QKD)** para alimentar algoritmos de cifrado clásicos.

El Flujo de Trabajo Híbrido:

- 1- **Generar Clave de Sesión (Cuántico):** Alice y Bob usan BB84 para generar de forma segura una clave relativamente corta (ej: 256 bits).
- 2- **Cifrar el Mensaje (Clásico):** Usan esa clave de 256 bits para un algoritmo de cifrado simétrico rápido y robusto, como **AES**, para cifrar el mensaje real.
- 3- **Enviar Mensaje Cifrado (Clásico):** El mensaje cifrado se envía por un canal de internet normal.

> **BB84 no reemplaza el cifrado clásico, sino que soluciona su mayor debilidad: la distribución segura de la clave inicial.**

Revisa la Sección 3 del cuaderno jupyter

clase10-qiskit.ipynb