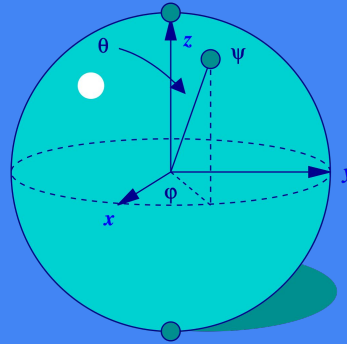


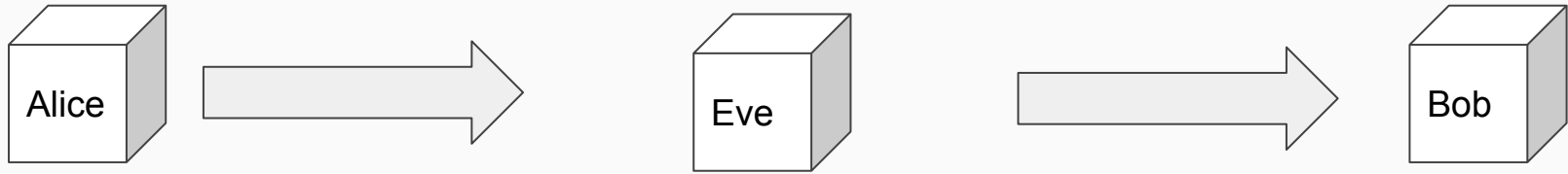
QKD BB84

Quantum Key Distribution



$$\left\{ \begin{array}{l} |0\rangle \\ |1\rangle \\ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{array} \right.$$

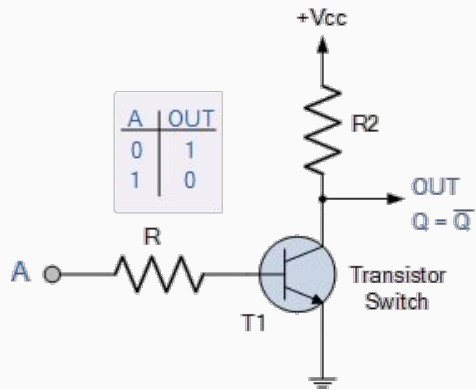
Alice & Bob (& Eve)



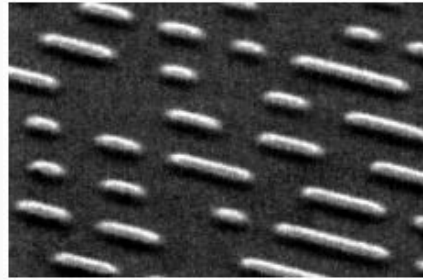
- PKI: Public Key Infrastructure
- DH: Diffie-Hellman
- PGP: Pretty Good Privacy
- <insert asymmetric protocol>

Bits - 0 y 1

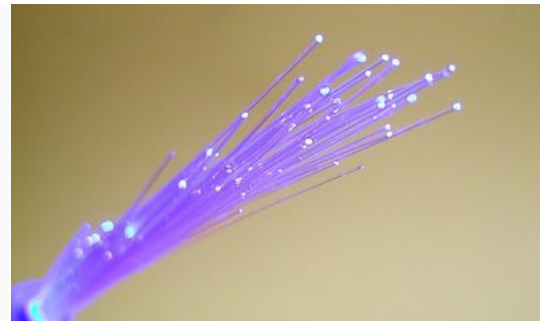
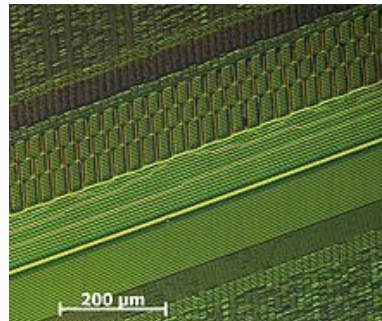
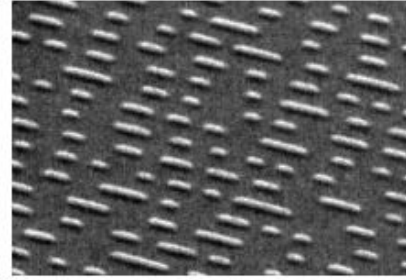
Física Electromagnética



CD



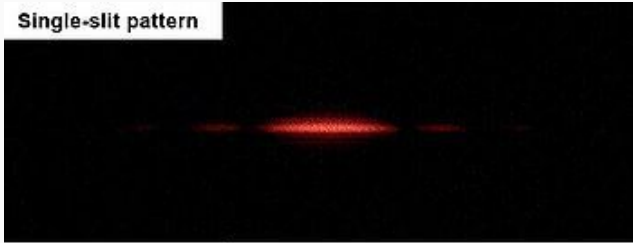
DVD



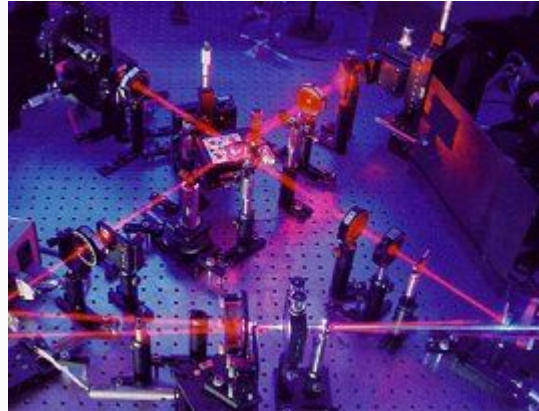
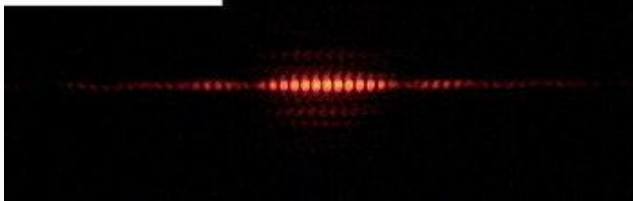
Qubits - $|0\rangle$ y $|1\rangle$

Física Cuántica

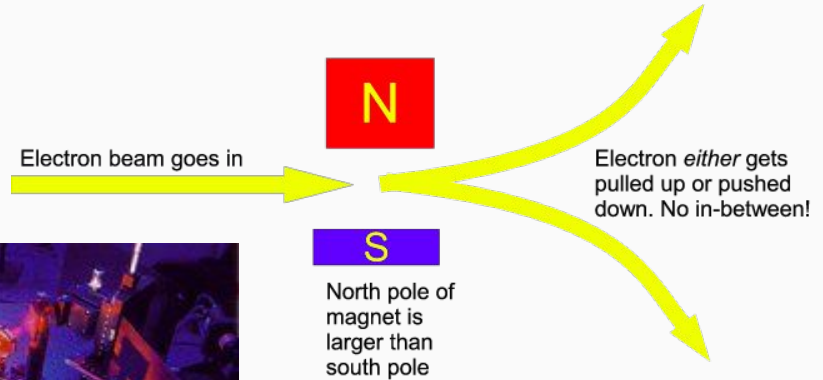
Single-slit pattern



Double-slit pattern



Electron beam goes in




North pole of magnet is larger than south pole

Superposiciones

$$\begin{array}{l} |0\rangle \\ |1\rangle \end{array} \left. \vphantom{\begin{array}{l} |0\rangle \\ |1\rangle \end{array}} \right\} \text{Estos son} \\ \text{Qubits}$$

¡Estos también
son Qubits!

$$\begin{array}{l} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{array}$$


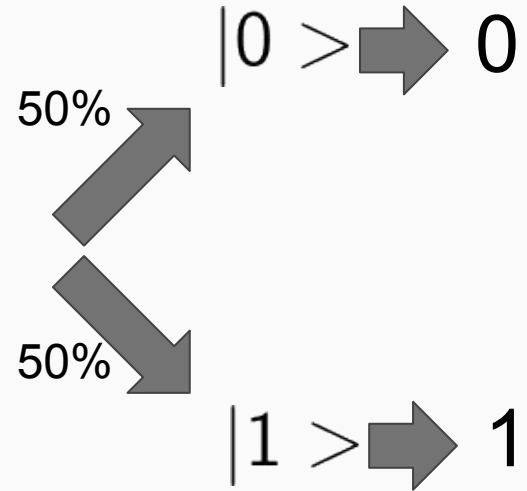
Ambos estados se “unen” en uno solo.
¡Ahora es otro estado distinto!

Superposiciones

Mide con base errónea.

$$\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \longrightarrow$$

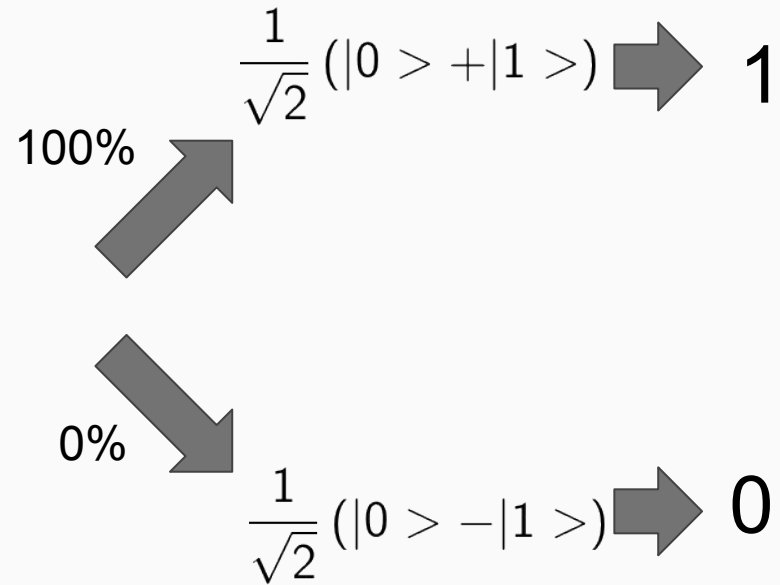
¿Sos $|1\rangle$?



Superposiciones

Mide con base correcta.

$$\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \longrightarrow \text{¿Sos } |0\rangle + |1\rangle?$$

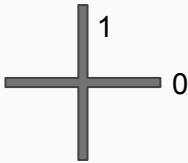


BB84

- Inventado por Charles Bennett y Gilles Brassard en 1984.
- Primer protocolo de intercambio de claves por medios cuánticos.
- Alice y Bob se comunican por Internet y por un canal cuántico.
 - Fibra optica.
 - Radiofrecuencia.
- Permite detectar un espía en el canal cuántico o canal clásico (no en ambos).

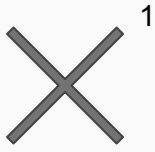
BB84 - Paso 1

- Alice genera N bits, para el bit 0 asigna una base cuántica y para el bit 1 asigna una base cuántica distinta.

$$0 \left\{ \begin{array}{l} |0\rangle \\ |1\rangle \end{array} \right.$$


A diagram showing a vertical line labeled '1' and a horizontal line labeled '0' intersecting at their centers. An upward-pointing arrow is positioned below the intersection.

Polarización
vertical/horizontal

$$1 \left\{ \begin{array}{l} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{array} \right.$$


A diagram showing two diagonal lines intersecting at their centers. The top-left line is labeled '0' and the bottom-right line is labeled '1'. An upward-pointing arrow is positioned below the intersection.

Polarización
diagonal

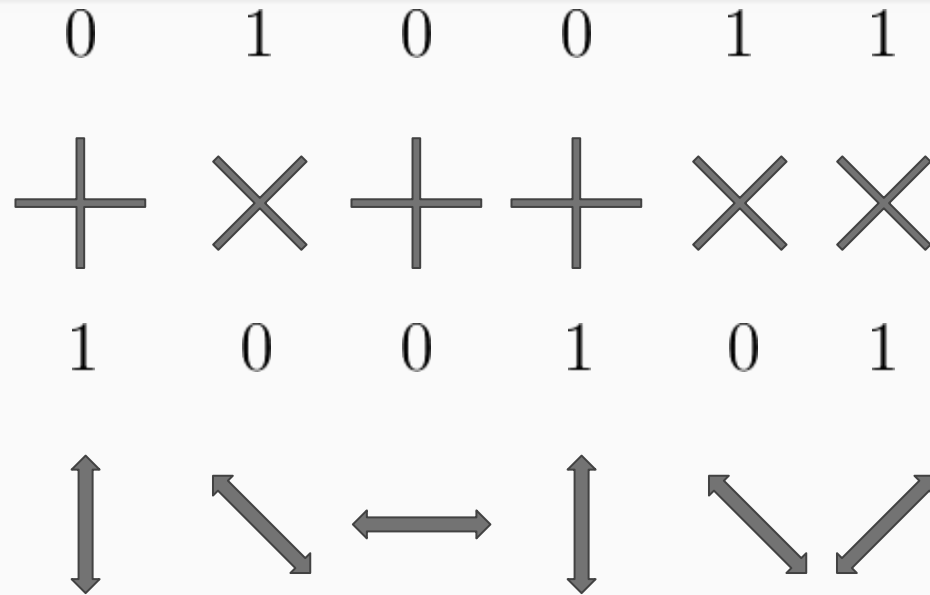
BB84 - Paso 1 - Ejemplo

0	1	0	0	1	1
+	×	+	+	×	×

BB84 - Paso 2

- Alice genera otros N bits aleatoriamente, donde hay un 0 asigna el estado cuántico asociado con 0 y donde hay un 1 asigna el estado cuántico asociado con 1.
- Alice transmite a Bob estos estados cuánticos.

BB84 - Paso 2 - Ejemplo



BB84 - Paso 3

- Bob genera N bits aleatorios y los asocia a bases cuánticas, tal como hizo Alice en el paso 1.

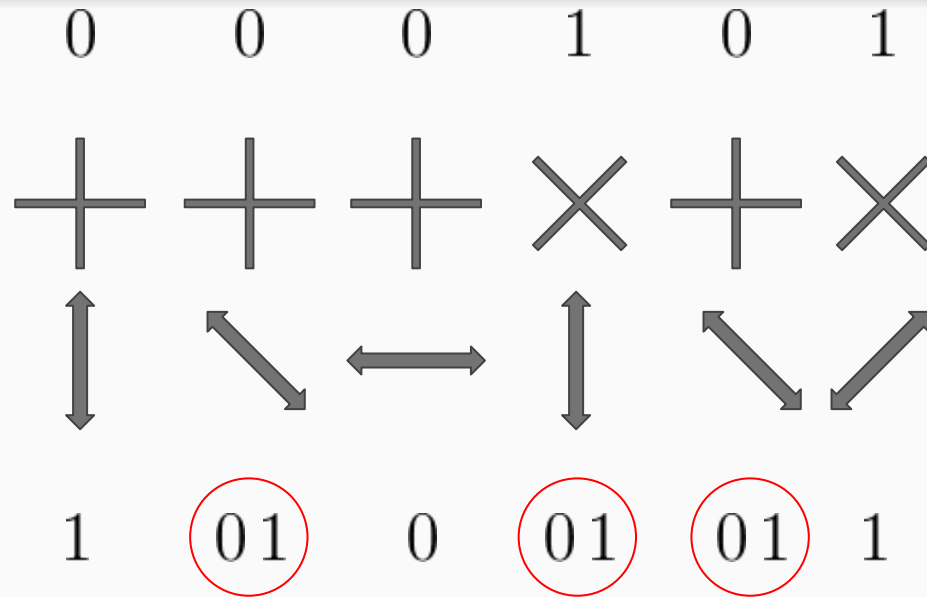
BB84 - Paso 3 - Ejemplo

0 0 0 1 0 1
+ + + × + ×

BB84 - Paso 4

- Bob mide cada Qubit que Alice le manda con sus bases, algunas veces va a coincidir en la base y mide correctamente, y otras veces no va a coincidir la base y mide incorrectamente.

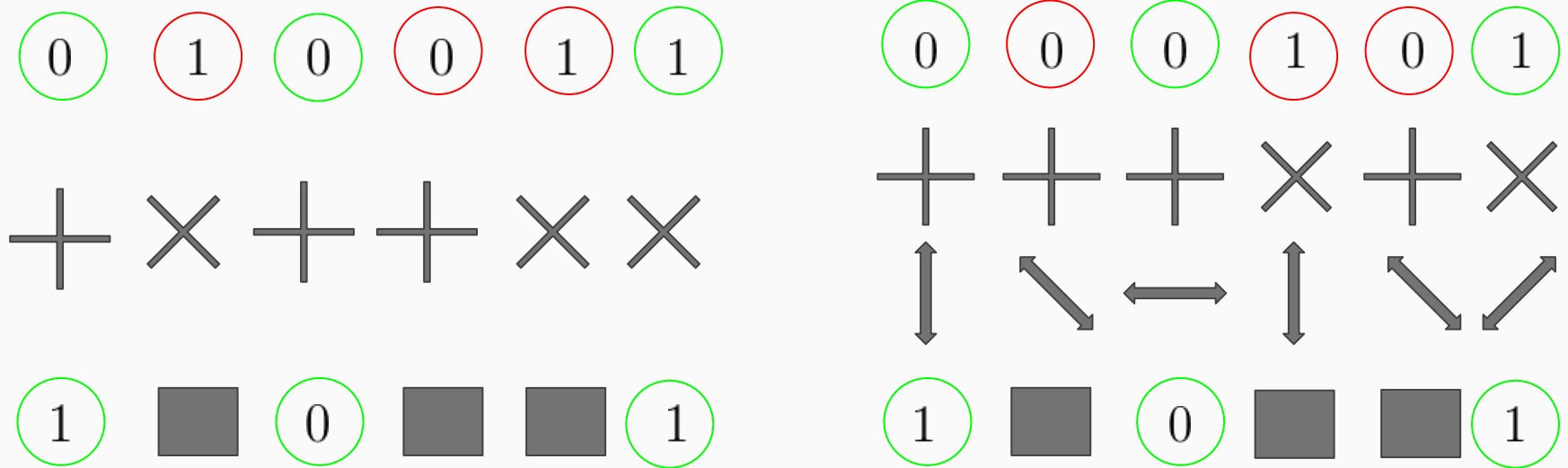
BB84 - Paso 4 - Ejemplo



BB84 - Paso 5

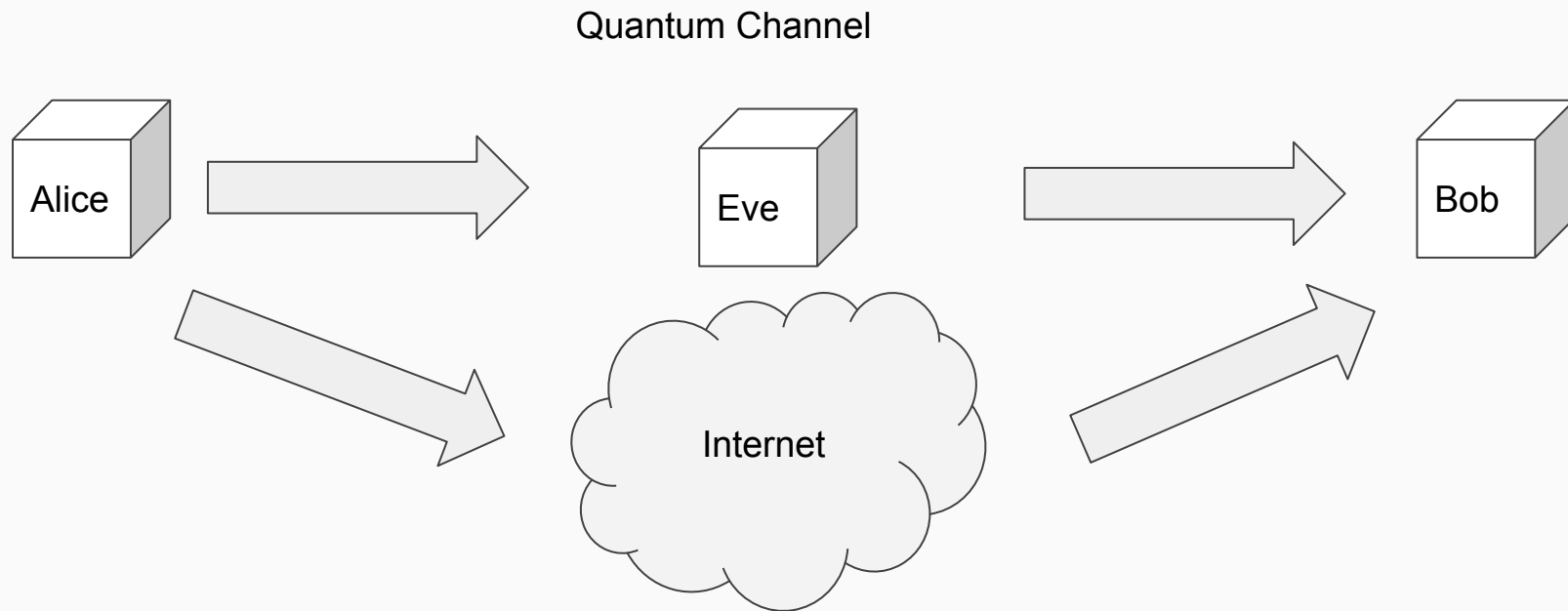
- Alice y Bob intercambian sus bases por Internet, comparan cuales coincidieron y cuáles no. De las bases que coinciden guardan los bits medidos, de las que no coinciden los descartan como inválidos.

BB84 - Paso 5 - Ejemplo



Key: 101

Eve



Eve

- Eve recibe los Qubits de Alice, tiene que adivinar las bases.
- Eve tiene que transmitir Qubits a Bob (supone que sus bases son correctas).
- Cuando Alice y Bob intercambien bases se van a dar cuenta que de las bases que coinciden los bits medidos son incorrectos.
- La probabilidad de tener al menos 1 bit erróneo aumenta con la cantidad de Qubits intercambiados (N).

Demo

- Se puede simular Qubits con un script de Python.
- <https://github.com/videlanicolas/QKD>
- La computadora clásica “juega” a ser una computadora cuántica.

QKD en la práctica

- 2003: USA (BBN Laboratories) -> Prueba funcional
- 2004-2008: Union Europea (SECOQC) -> Red entre SIEMENS
- 2009: Suiza (Universidad de Ginebra) -> Prueba comercial
- 2016: China (Satélite Micius) -> Prueba QKD en el espacio



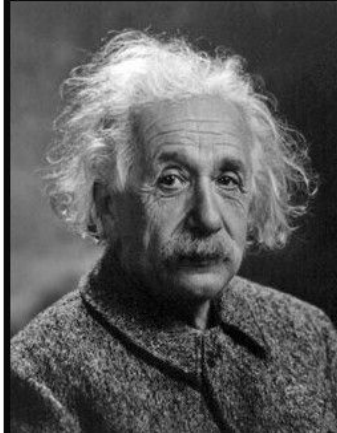
I think I can safely say that nobody understands
quantum mechanics.

(Richard Feynman)

izquotes.com

¿Preguntas?

¡Gracias!



God does not play dice.

(Albert Einstein)

izquotes.com