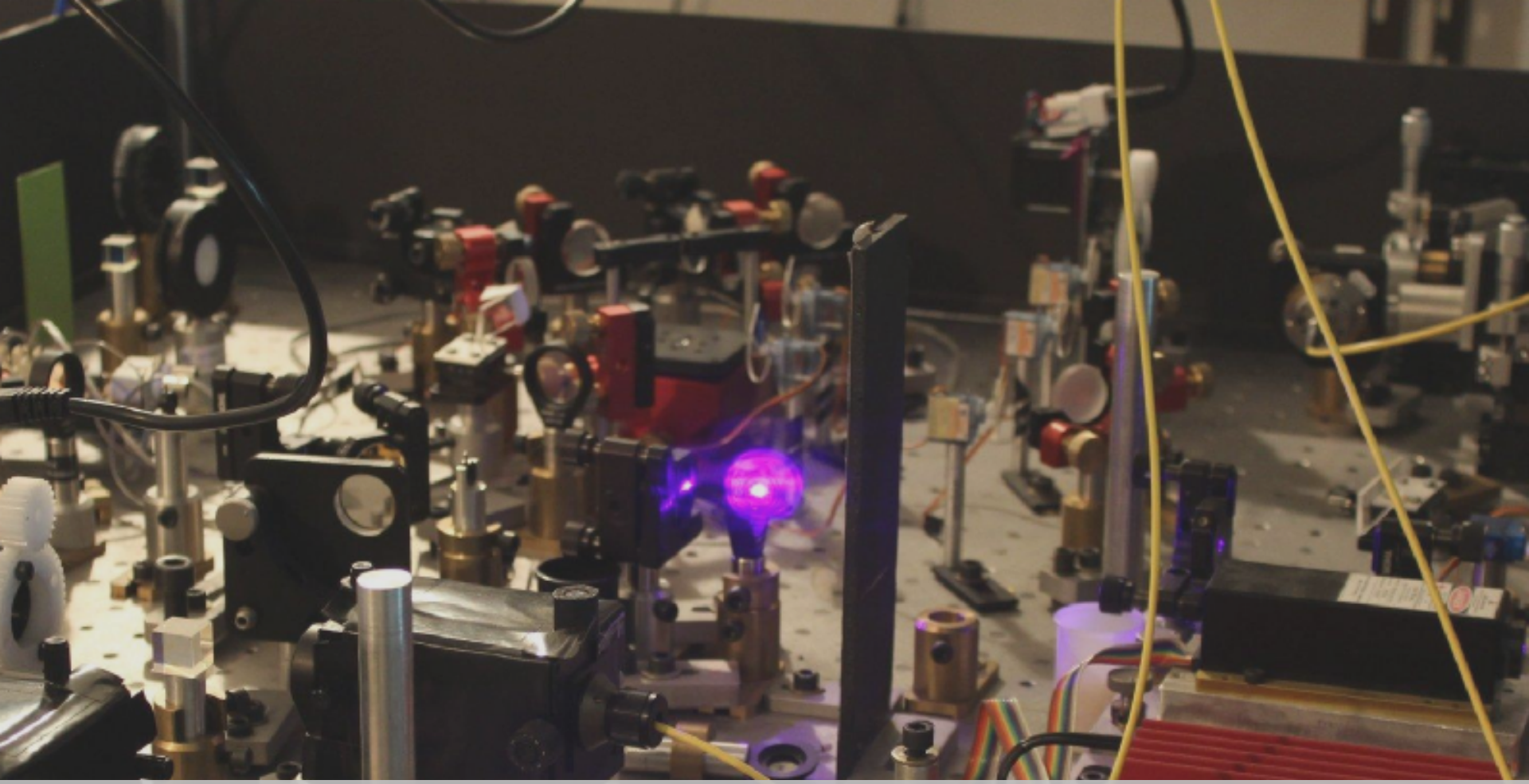


Experimentos con fotones entrelazados

Laura T. Knoll
Laboratorio de Óptica Cuántica
(DEILAP-CITEDEF)

7 de Junio de 2018

Estructura de la charla

Introducción

- Codificación de qubits en grados de libertad de un fotón
- Generación de pares de fotones entrelazados en polarización

Teleportación cuántica

- Implementación fotónica y resultados

Distribución cuántica de claves

- Implementación fotónica
- Espionaje con una máquina de clonación

Introducción

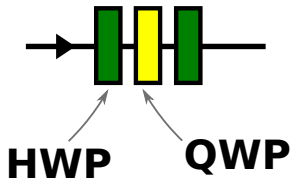
Codificación de qubits en GDL del fotón

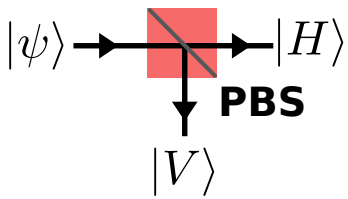
Qubits de polarización

$$\left.\begin{array}{l}|0\rangle \rightarrow |H\rangle \\ |1\rangle \rightarrow |V\rangle\end{array}\right\} \quad |\psi\rangle = \alpha|H\rangle + \beta|V\rangle$$

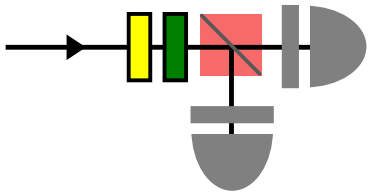
Qubit	Estado de Polarización	Nombre
$\|0\rangle$	$\|H\rangle$	Horizontal
$\|1\rangle$	$\|V\rangle$	Vertical
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|D\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	Diagonal
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|A\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	Antidiagonal
$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	Circular Izquierda
$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	Circular Derecha

Generación y manipulación





Detección (Tomografía de estados QST)



Qubits de camino

$$P_{\phi_1} \cdot BS \cdot P_{\phi_2} \cdot BS^\dagger \cdot P_{\phi_3} =$$

$$= e^{i\phi_2/2} \begin{pmatrix} e^{i(\phi_1+\phi_3)}\cos(\phi_2/2) & e^{i\phi_3}\sin(\phi_2/2) \\ -e^{i\phi_1}\sin(\phi_2/2) & \cos(\phi_2/2) \end{pmatrix}$$

Introducción

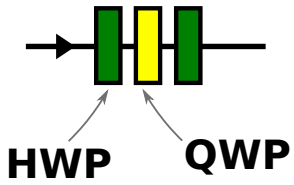
Codificación de qubits en GDL del fotón

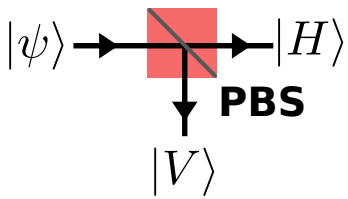
Qubits de polarización

$$\left.\begin{array}{l}|0\rangle \rightarrow |H\rangle \\ |1\rangle \rightarrow |V\rangle\end{array}\right\} \quad |\psi\rangle = \alpha|H\rangle + \beta|V\rangle$$

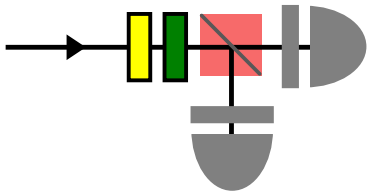
Qubit	Estado de Polarización	Nombre
$\|0\rangle$	$\|H\rangle$	Horizontal
$\|1\rangle$	$\|V\rangle$	Vertical
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|D\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	Diagonal
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|A\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	Antidiagonal
$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	Circular Izquierda
$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	Circular Derecha

Generación y manipulación

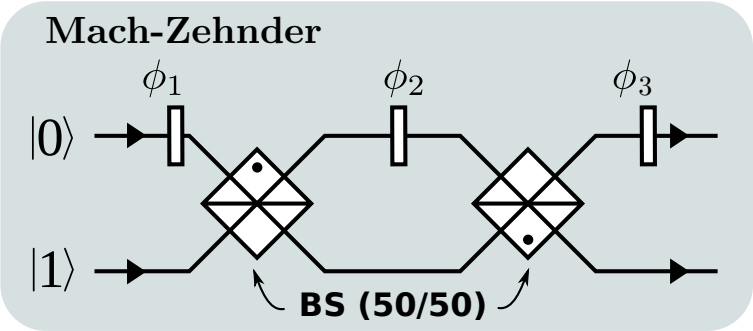




Detección (Tomografía de estados QST)



Qubits de camino



$$R = P_{\phi_1} \cdot BS \cdot P_{\phi_2} \cdot BS^\dagger \cdot P_{\phi_3} =$$

$$= e^{i\phi_2/2} \begin{pmatrix} e^{i(\phi_1+\phi_3)}\cos(\phi_2/2) & e^{i\phi_3}\sin(\phi_2/2) \\ -e^{i\phi_1}\sin(\phi_2/2) & \cos(\phi_2/2) \end{pmatrix}$$

Englert, Phys. Rev. A 63 (2001)

Ejemplos

$$\phi_1 = \phi_2 = \phi_3 = 0 \Rightarrow R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\phi_1 = 0, \phi_3 = \pi, \phi_2 = \pi/4 \Rightarrow R = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Introducción

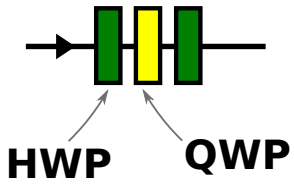
Codificación de qubits en GDL del fotón

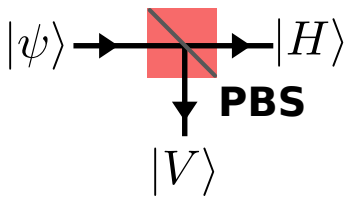
Qubits de polarización

$$\left.\begin{array}{l} |0\rangle \to |H\rangle \\ |1\rangle \to |V\rangle \end{array}\right\} \quad |\psi\rangle = \alpha|H\rangle + \beta|V\rangle$$

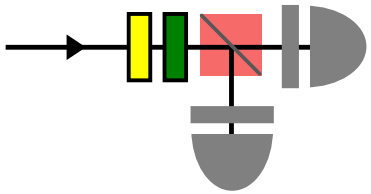
Qubit	Estado de Polarización	Nombre
$\|0\rangle$	$\|H\rangle$	Horizontal
$\|1\rangle$	$\|V\rangle$	Vertical
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|D\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	Diagonal
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|A\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	Antidiagonal
$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	Circular Izquierda
$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	Circular Derecha

Generación y manipulación

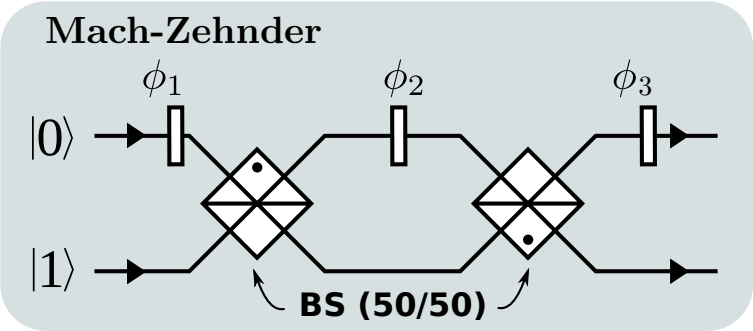




Detección (Tomografía de estados QST)

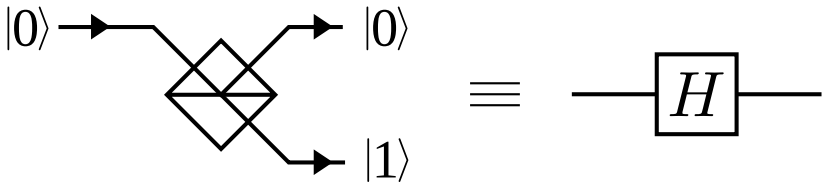


Qubits de camino



$$P_{\phi_1} \cdot BS \cdot P_{\phi_2} \cdot BS^\dagger \cdot P_{\phi_3} =$$

$$= e^{i\phi_2/2} \begin{pmatrix} e^{i(\phi_1+\phi_3)}\cos(\phi_2/2) & e^{i\phi_3}\sin(\phi_2/2) \\ -e^{i\phi_1}\sin(\phi_2/2) & \cos(\phi_2/2) \end{pmatrix}$$



Hadamard $\begin{cases} |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

Introducción

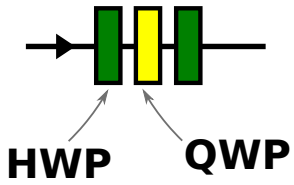
Codificación de qubits en GDL del fotón

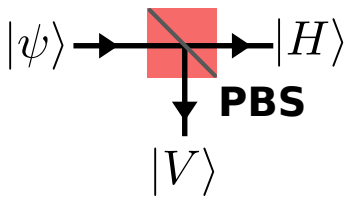
Qubits de polarización

$$\left.\begin{array}{l}|0\rangle \rightarrow |H\rangle \\ |1\rangle \rightarrow |V\rangle\end{array}\right\} \quad |\psi\rangle = \alpha|H\rangle + \beta|V\rangle$$

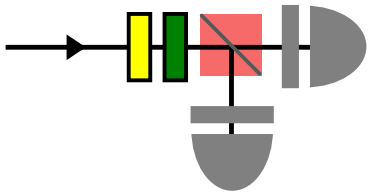
Qubit	Estado de Polarización	Nombre
$\|0\rangle$	$\|H\rangle$	Horizontal
$\|1\rangle$	$\|V\rangle$	Vertical
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|D\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	Diagonal
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|A\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	Antidiagonal
$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	Circular Izquierda
$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	Circular Derecha

Generación y manipulación

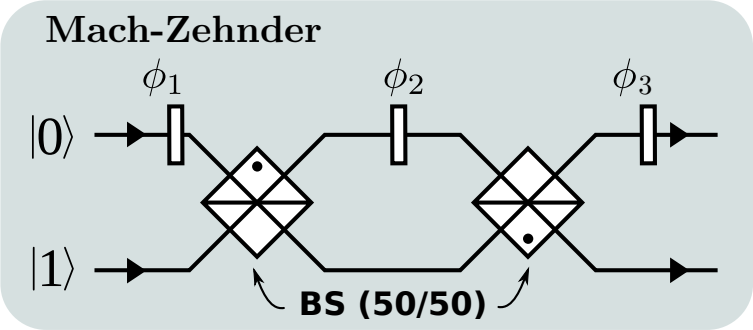




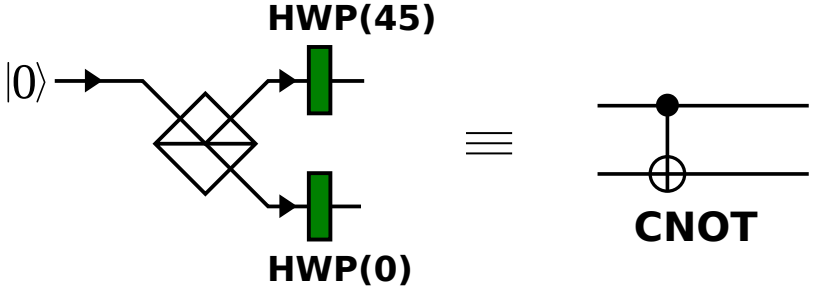
Detección (Tomografía de estados QST)



Qubits de camino



Operación controlada en camino y polarización



$$\textbf{CNOT} \left\{\begin{array}{l}|0H\rangle \rightarrow |0H\rangle \\ |0V\rangle \rightarrow |0V\rangle \\ |1H\rangle \rightarrow |1V\rangle \\ |1V\rangle \rightarrow |1H\rangle\end{array}\right.$$

Introducción

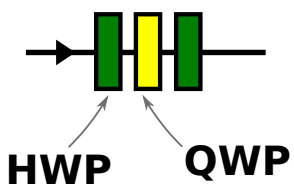
Codificación de qubits en GDL del fotón

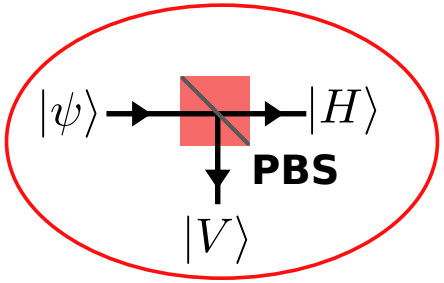
Qubits de polarización

$$\left.\begin{array}{l}|0\rangle \rightarrow |H\rangle \\ |1\rangle \rightarrow |V\rangle\end{array}\right\} \quad |\psi\rangle = \alpha|H\rangle + \beta|V\rangle$$

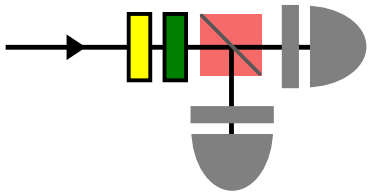
Qubit	Estado de Polarización	Nombre
$\|0\rangle$	$\|H\rangle$	Horizontal
$\|1\rangle$	$\|V\rangle$	Vertical
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|D\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	Diagonal
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|A\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	Antidiagonal
$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	Circular Izquierda
$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	Circular Derecha

Generación y manipulación

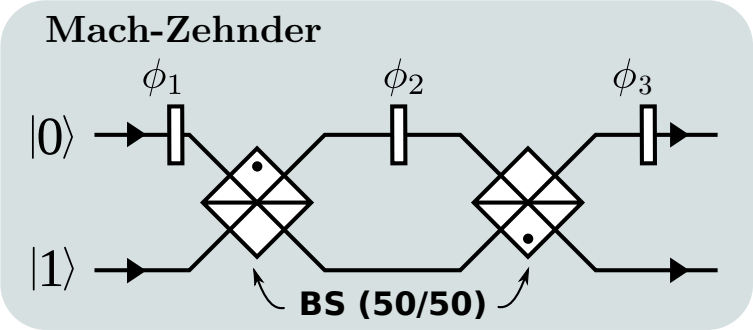




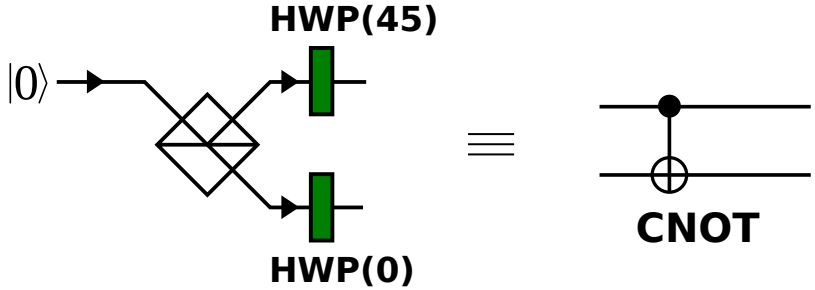
Detección (Tomografía de estados QST)



Qubits de camino



Operación controlada en camino y polarización



$$\textbf{CNOT} \left\{\begin{array}{l}|0H\rangle \rightarrow |0H\rangle \\ |0V\rangle \rightarrow |0V\rangle \\ |1H\rangle \rightarrow |1V\rangle \\ |1V\rangle \rightarrow |1H\rangle\end{array}\right.$$

Introducción

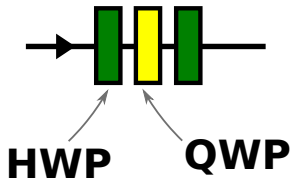
Codificación de qubits en GDL del fotón

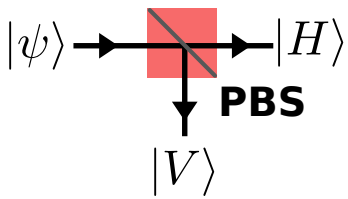
Qubits de polarización

$$\left.\begin{array}{l}|0\rangle \rightarrow |H\rangle \\ |1\rangle \rightarrow |V\rangle\end{array}\right\} \quad |\psi\rangle = \alpha|H\rangle + \beta|V\rangle$$

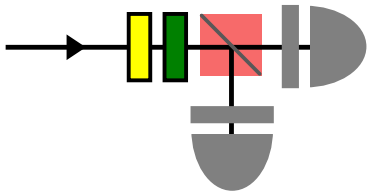
Qubit	Estado de Polarización	Nombre
$\|0\rangle$	$\|H\rangle$	Horizontal
$\|1\rangle$	$\|V\rangle$	Vertical
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|D\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	Diagonal
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|A\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	Antidiagonal
$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	Circular Izquierda
$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	Circular Derecha

Generación y manipulación

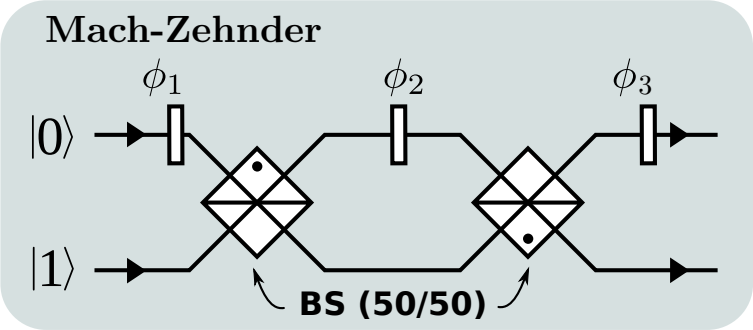


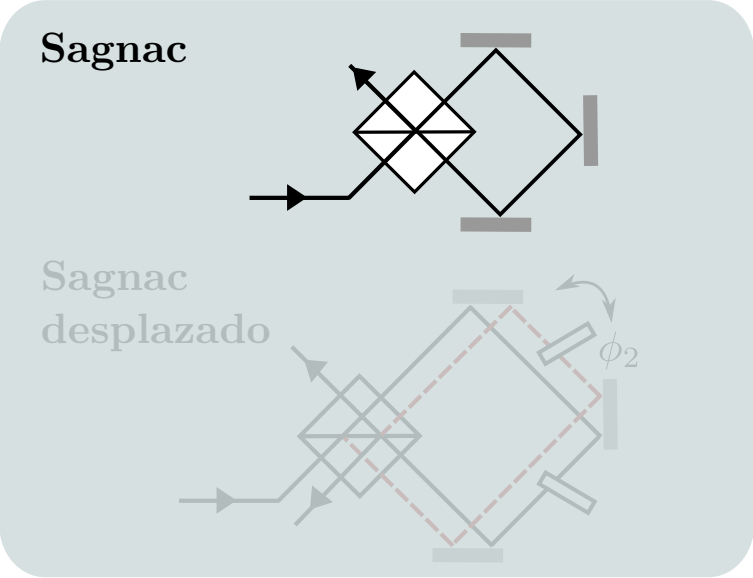


Detección (Tomografía de estados QST)



Qubits de camino





Introducción

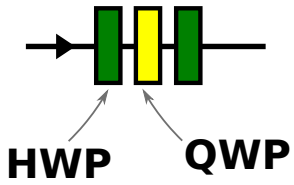
Codificación de qubits en GDL del fotón

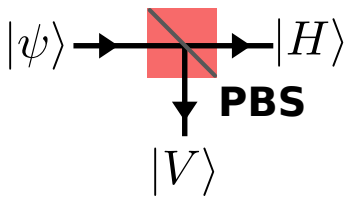
Qubits de polarización

$$\left.\begin{array}{l}|0\rangle \rightarrow |H\rangle \\ |1\rangle \rightarrow |V\rangle\end{array}\right\} \quad |\psi\rangle = \alpha|H\rangle + \beta|V\rangle$$

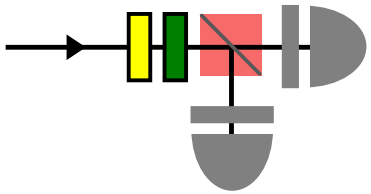
Qubit	Estado de Polarización	Nombre
$\|0\rangle$	$\|H\rangle$	Horizontal
$\|1\rangle$	$\|V\rangle$	Vertical
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|D\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	Diagonal
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|A\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	Antidiagonal
$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	Circular Izquierda
$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	Circular Derecha

Generación y manipulación

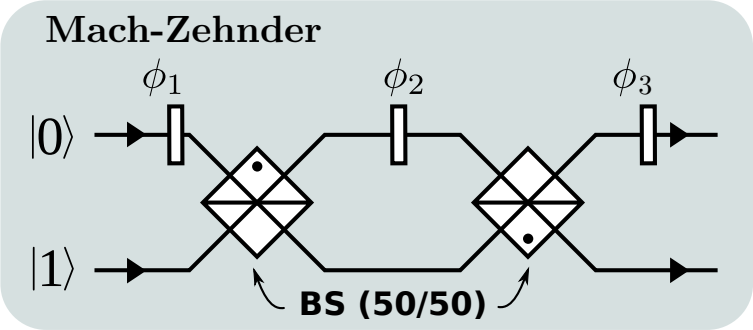


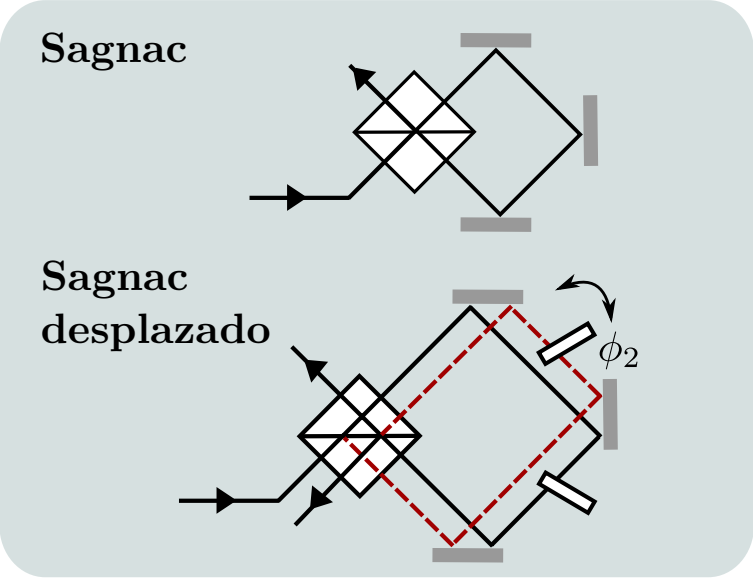


Detección (Tomografía de estados QST)



Qubits de camino





Introducción

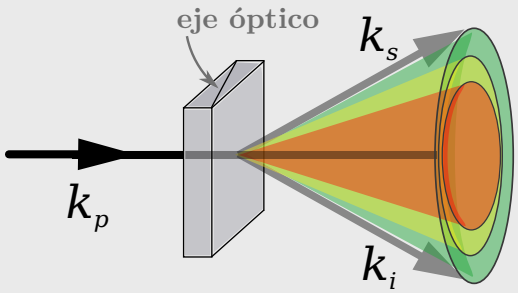
Generación de fotones entrelazados en polarización

Fluorecencia paramétrica descendente (SPDC)

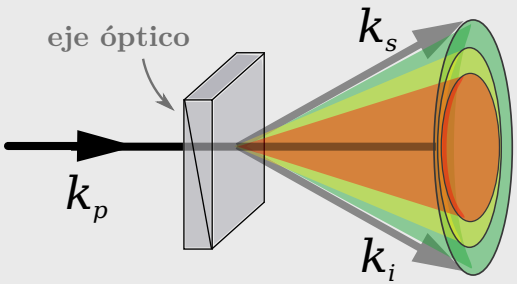
$p : pump$
$s : signal$
$i : idler$

$$\omega_p = \omega_s + \omega_i, \quad \boldsymbol{k}_p = \boldsymbol{k}_s + \boldsymbol{k}_i$$

Tipo I: correlación en la polarización $\quad e \rightarrow o + o$



$|H\rangle \rightarrow |VV\rangle$



$|V\rangle \rightarrow |HH\rangle$

PG Kwiat, Phys. Rev. A 60 (1999)

Introducción

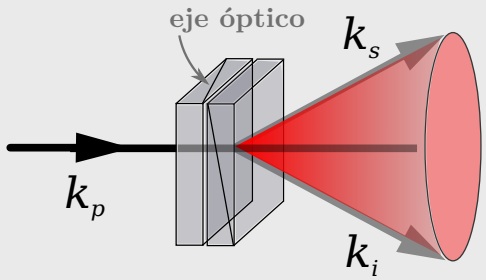
Generación de fotones entrelazados en polarización

Fluorecencia paramétrica descendente (SPDC)

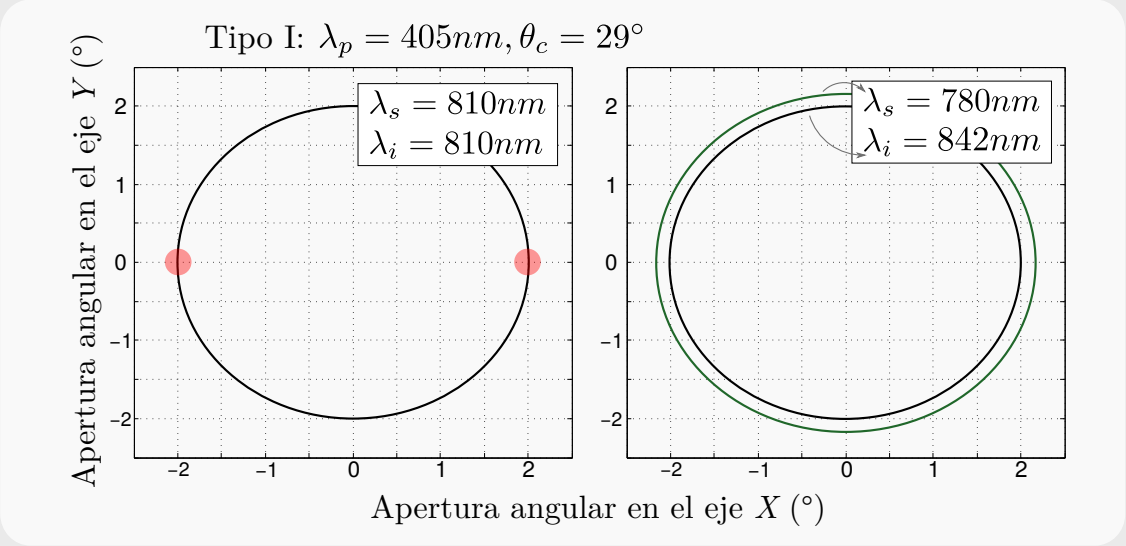
$$\omega_p = \omega_s + \omega_i, \quad \boldsymbol{k}_p = \boldsymbol{k}_s + \boldsymbol{k}_i$$

$p : pump$
$s : signal$
$i : idler$

Tipo I



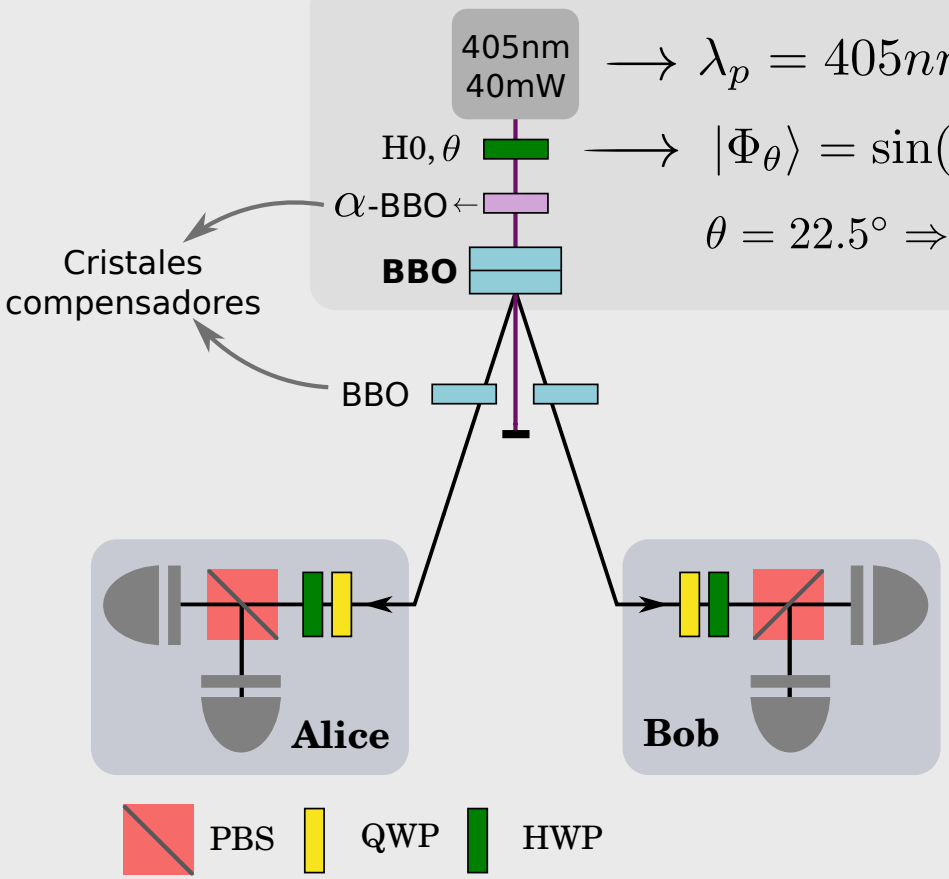
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + e^{i\phi}|VV\rangle)$$



PG Kwiat, Phys. Rev. A 60 (1999)

Introducción

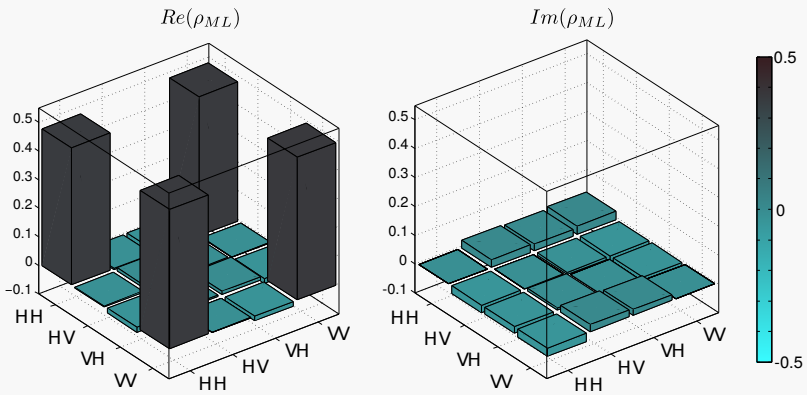
Fuente de pares de fotones entrelazados en polarización



$$\longrightarrow \lambda_p = 405nm \Rightarrow \lambda_s = \lambda_i = 810nm$$

$$\longrightarrow |\Phi_\theta\rangle = \sin(2\theta)|HH\rangle + \cos(2\theta)|VV\rangle$$

$$\theta = 22.5^\circ \Rightarrow |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$$



Fidelidad $F = 0.95 \pm 0.01$

Valor de S (CHSH) $S = 2.703 \pm 0.067$

Estructura de la charla

Introducción

- Generación de pares de fotones entrelazados en polarización
- Codificación de qubits en grados de libertad de un fotón

Teleportación cuántica

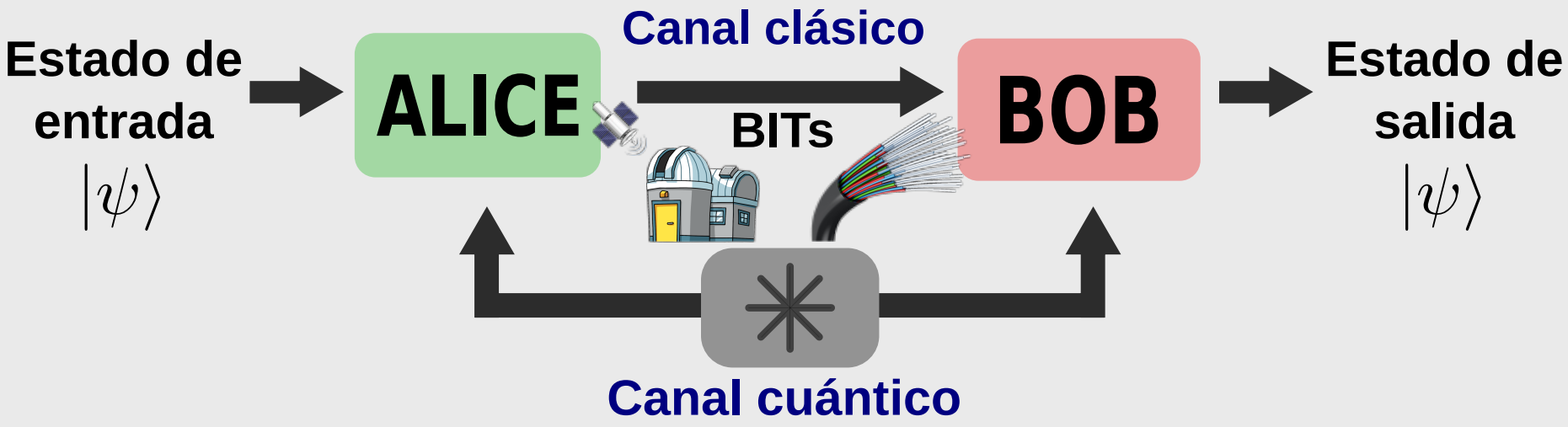
- Implementación fotónica y resultados

Distribución cuántica de claves

- Implementación fotónica
- Espionaje con una máquina de clonación

Teleportación cuántica

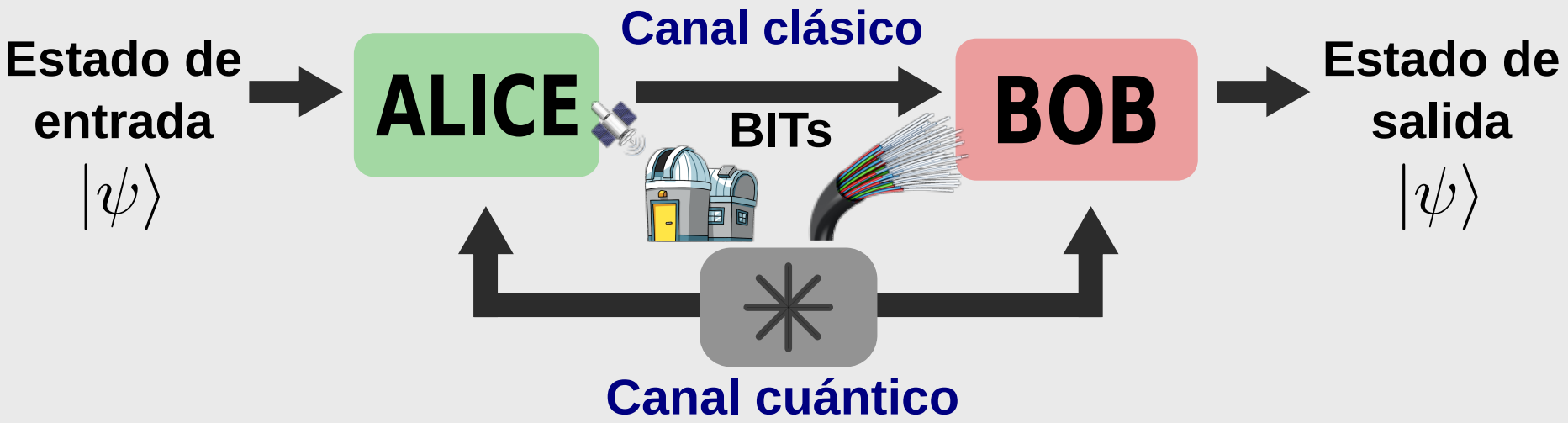
El algoritmo



CH Bennett, G Brassard, et. al., Phys. Rev. Lett. 70 (1993)

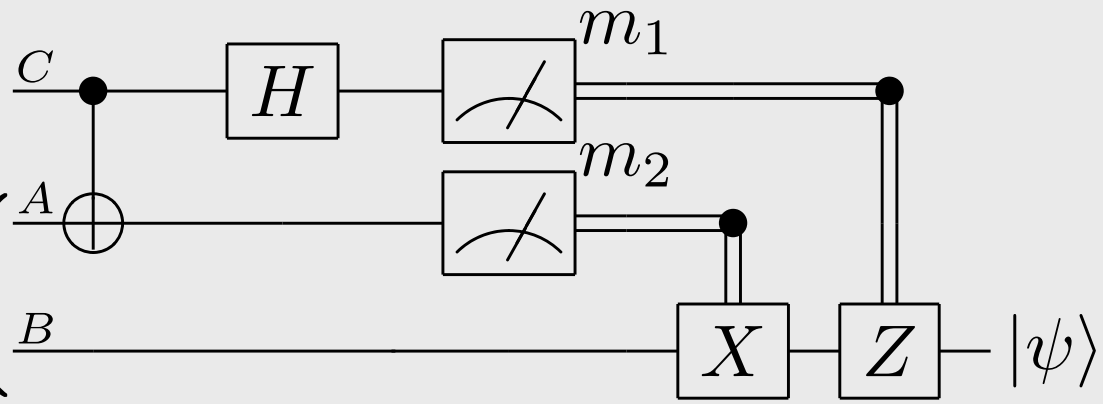
Teleportación cuántica

El algoritmo



$$|\psi\rangle_C = \alpha\,|0\rangle + \beta\,|1\rangle$$

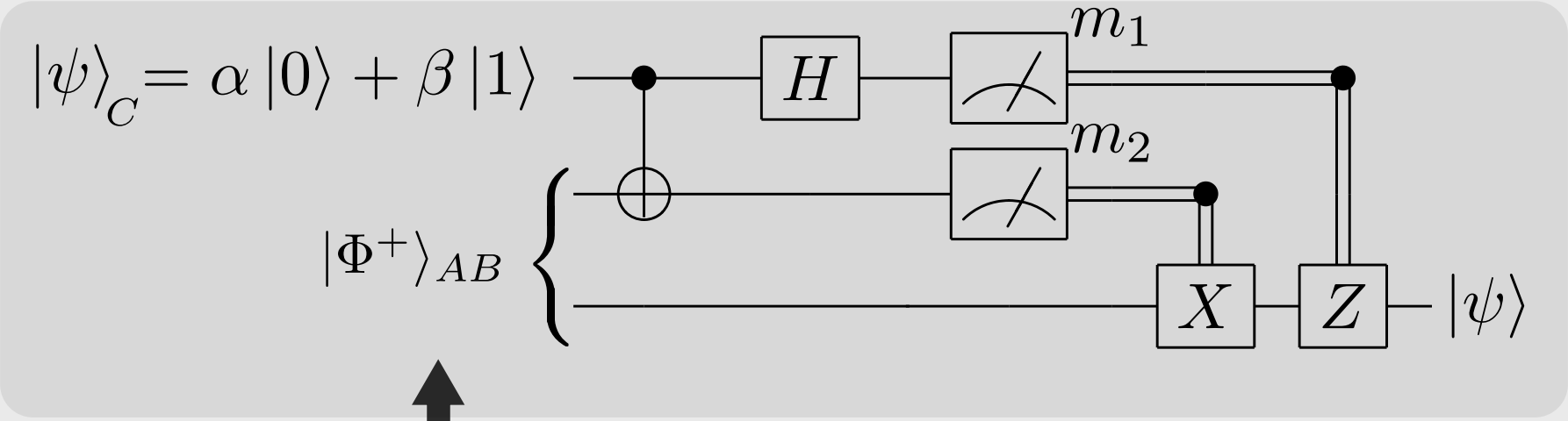
$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$$



CH Bennett, G Brassard, et. al., Phys. Rev. Lett. 70 (1993)

Teleportación cuántica

El algoritmo

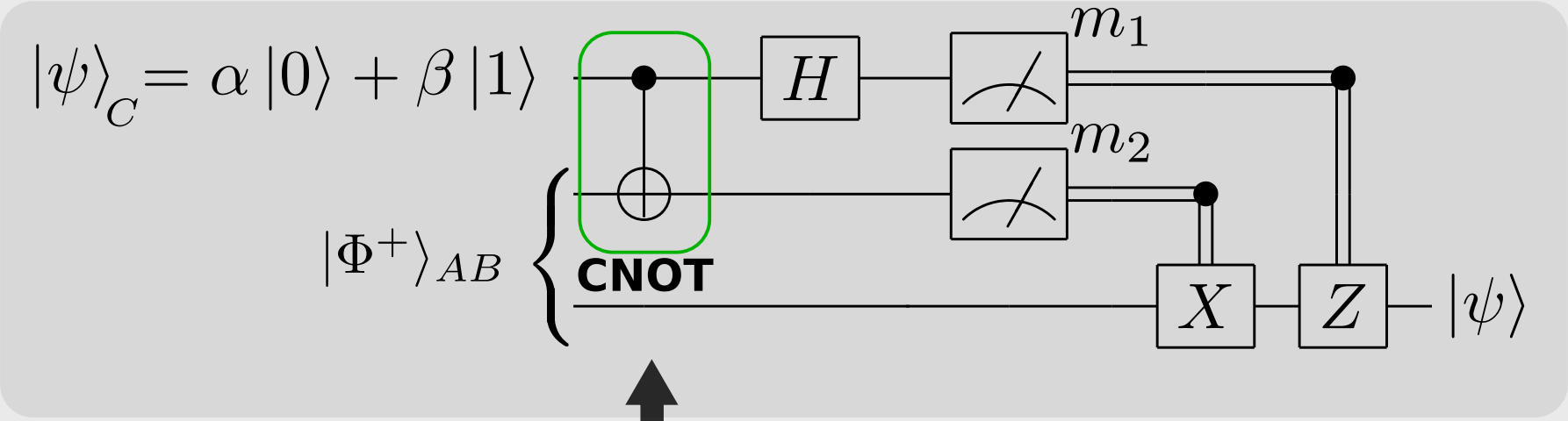


$$|\psi_0\rangle_{CAB} = |\psi\rangle_C |\Phi^+\rangle_{AB}$$ **Estado inicial**

$$|\psi_0\rangle_{CAB} = \frac{1}{\sqrt{2}}[\alpha|0\rangle_C(|00\rangle_{AB} + |11\rangle_{AB}) + \beta|1\rangle_C(|00\rangle_{AB} + |11\rangle_{AB})]$$

Teleportación cuántica

El algoritmo



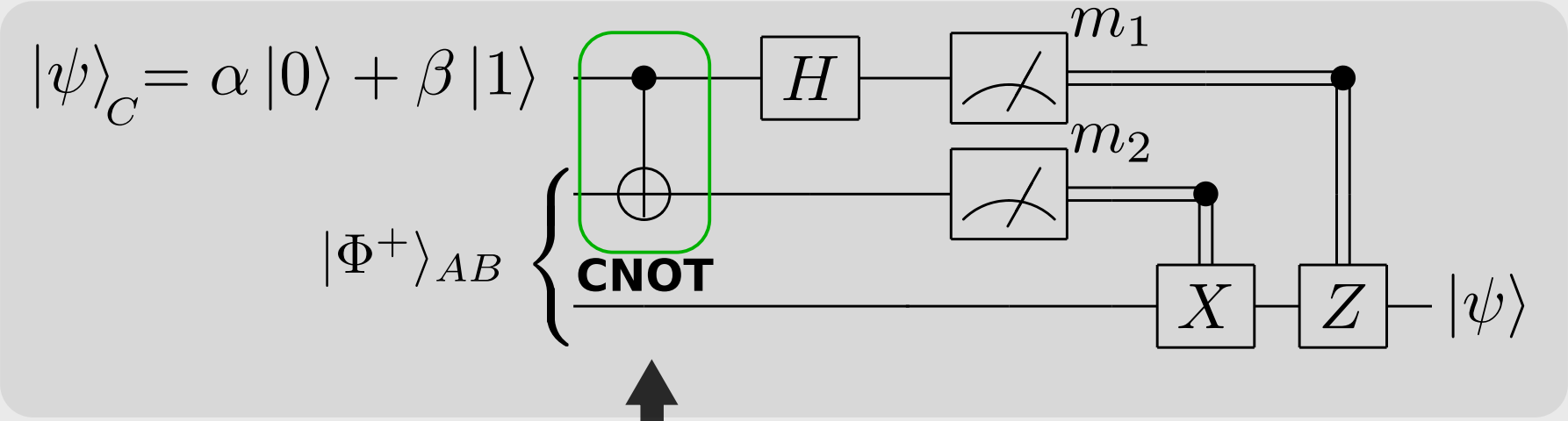
$|\psi_1\rangle_{CAB}$

CNOT $\begin{cases} |00\rangle_{CA} \to |00\rangle_{CA} \\ |01\rangle_{CA} \to |01\rangle_{CA} \\ |10\rangle_{CA} \to |11\rangle_{CA} \\ |11\rangle_{CA} \to |10\rangle_{CA} \end{cases}$

$$|\psi_0\rangle_{CAB} = \frac{1}{\sqrt{2}}[\alpha|0\rangle_C(|00\rangle_{AB} + |11\rangle_{AB}) + \beta|1\rangle_C(|00\rangle_{AB} + |11\rangle_{AB})]$$

Teleportación cuántica

El algoritmo



$|\psi_1\rangle_{CAB}$

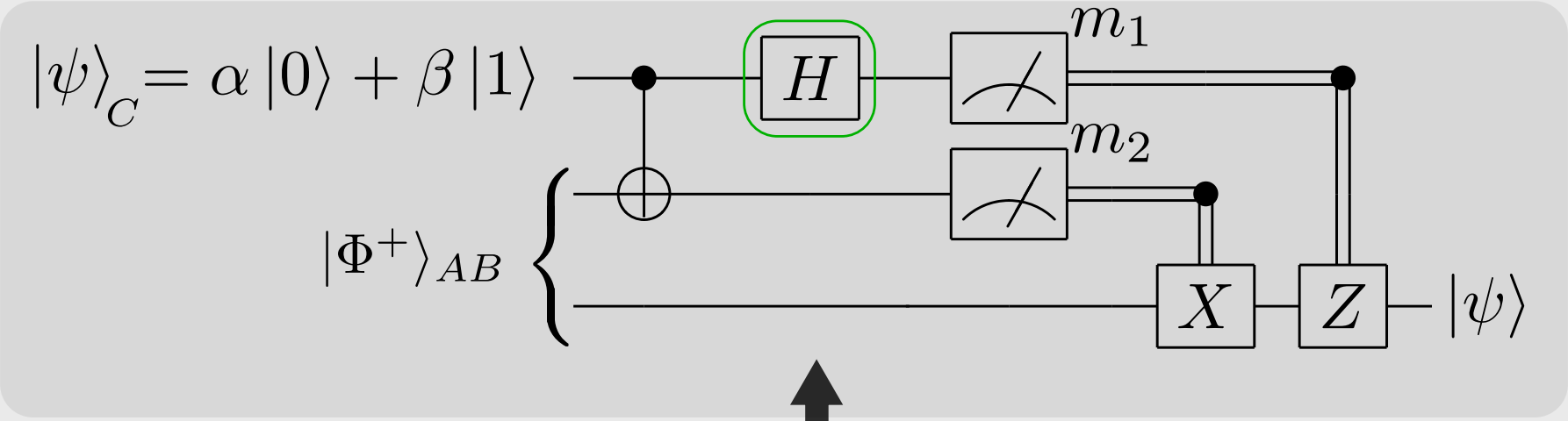
CNOT $\begin{cases} |00\rangle_{CA} \to |00\rangle_{CA} \\ |01\rangle_{CA} \to |01\rangle_{CA} \\ |10\rangle_{CA} \to |11\rangle_{CA} \\ |11\rangle_{CA} \to |10\rangle_{CA} \end{cases}$

$$|\psi_0\rangle_{CAB} = \frac{1}{\sqrt{2}}[\alpha|0\rangle_C(|00\rangle_{AB} + |11\rangle_{AB}) + \beta|1\rangle_C(|00\rangle_{AB} + |11\rangle_{AB})]$$

$$|\psi_1\rangle_{CAB} = \frac{1}{\sqrt{2}}[\alpha|0\rangle_C(|00\rangle_{AB} + |11\rangle_{AB}) + \beta|1\rangle_C(|10\rangle_{AB} + |01\rangle)_{AB}]$$

Teleportación cuántica

El algoritmo



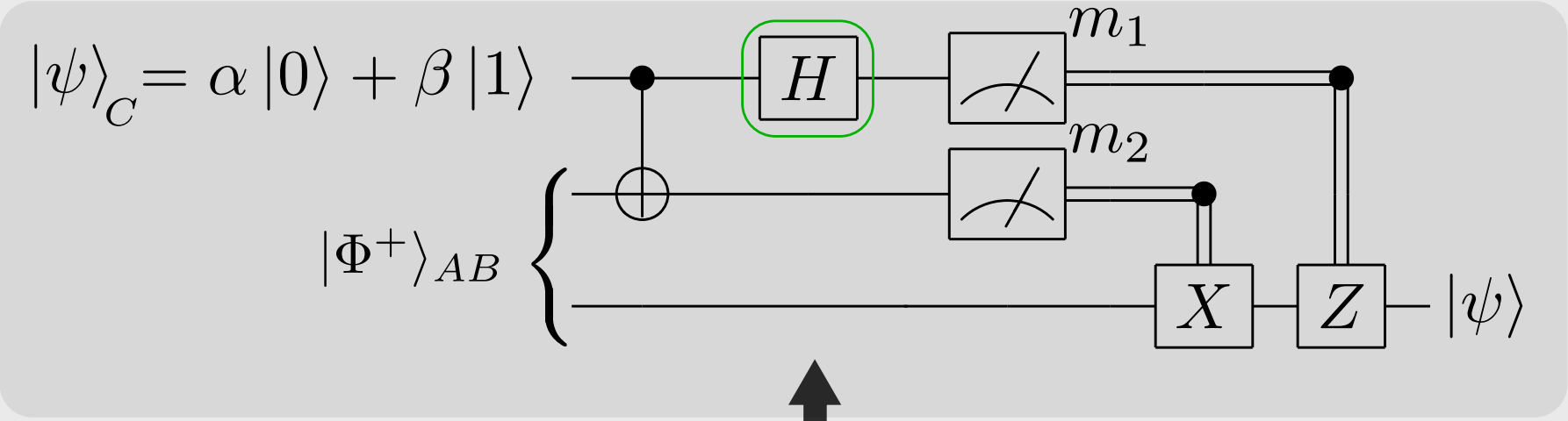
$|\psi_2\rangle_{CAB}$

Hadamard $\begin{cases} |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

$$|\psi_1\rangle_{CAB} = \frac{1}{\sqrt{2}}[\alpha|0\rangle_C(|00\rangle_{AB} + |11\rangle_{AB}) + \beta|1\rangle_C(|10\rangle_{AB} + |01\rangle)_{AB}]$$

Teleportación cuántica

El algoritmo



$|\psi_2\rangle_{CAB}$

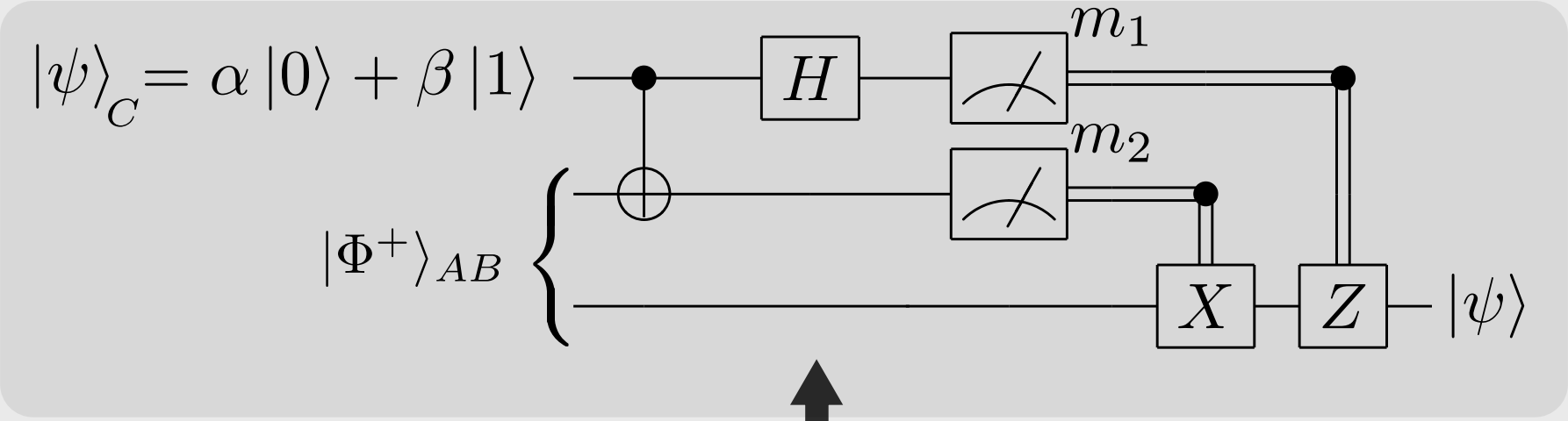
Hadamard $\begin{cases} |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

$$|\psi_1\rangle_{CAB} = \frac{1}{\sqrt{2}}[\alpha|0\rangle_C(|00\rangle_{AB} + |11\rangle_{AB}) + \beta|1\rangle_C(|10\rangle_{AB} + |01\rangle)_{AB}]$$

$$|\psi_2\rangle_{CAB} = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)_C(|00\rangle_{AB} + |11\rangle_{AB}) + \beta(|0\rangle - |1\rangle)_C(|10\rangle_{AB} + |01\rangle_{AB})]$$

Teleportación cuántica

El algoritmo

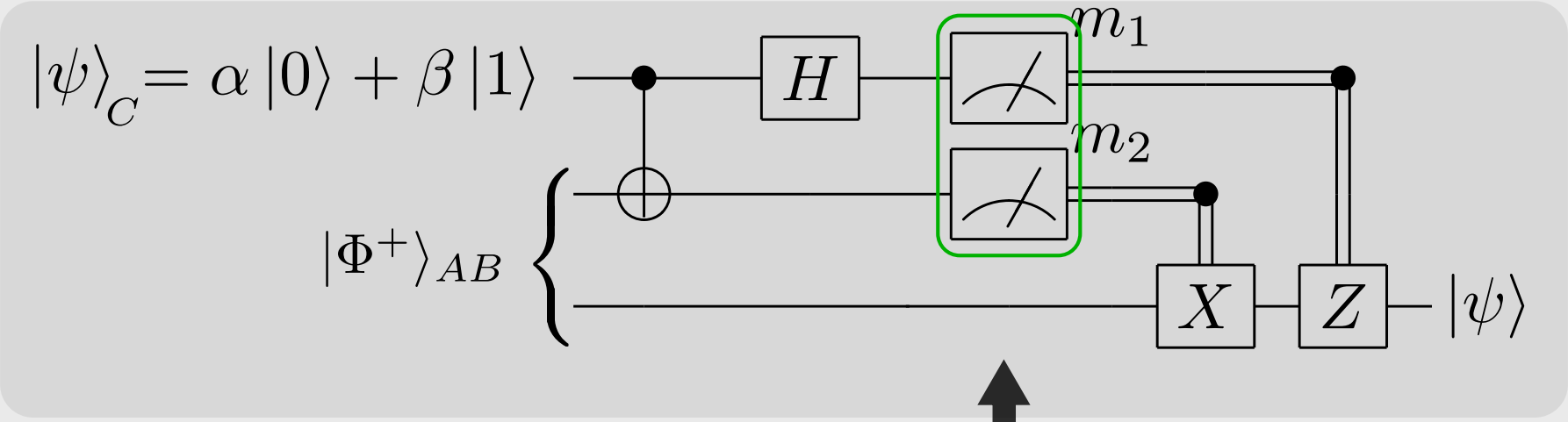


$$|\psi_2\rangle_{CAB}$$

$$\begin{aligned}|\psi_2\rangle_{CAB} = \tfrac{1}{2}[&|00\rangle_{CA}(\alpha|0\rangle + \beta|1\rangle)_B + \\ &|01\rangle_{CA}(\alpha|1\rangle + \beta|0\rangle)_B + \\ &|10\rangle_{CA}(\alpha|0\rangle - \beta|1\rangle)_B + \\ &|11\rangle_{CA}(\alpha|1\rangle - \beta|0\rangle)_B]\end{aligned}$$

Teleportación cuántica

El algoritmo

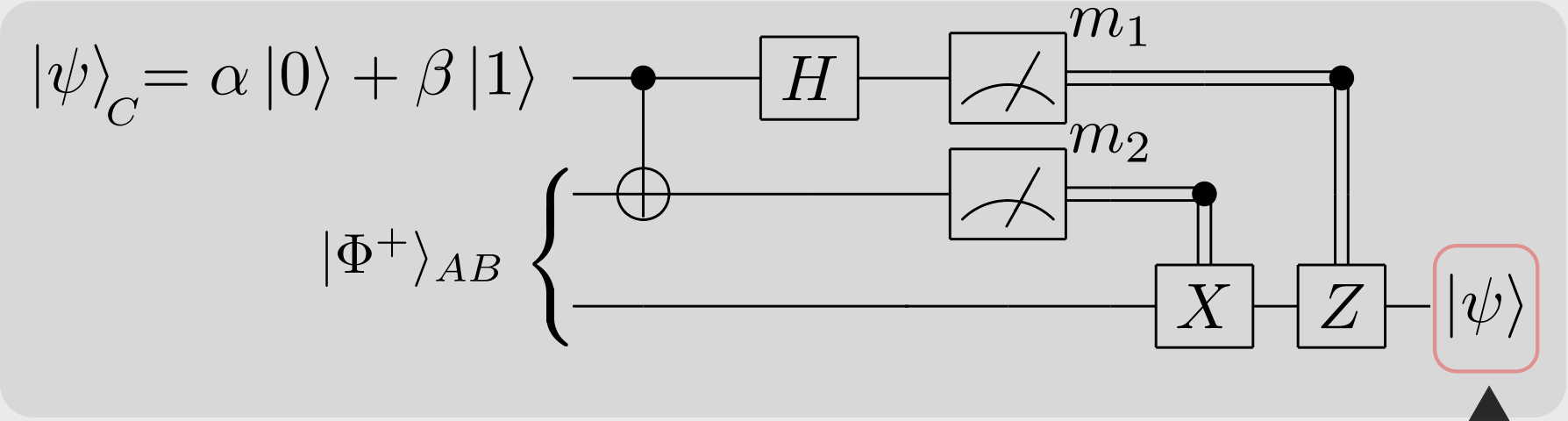


Alice realiza una medida proyectiva sobre sus dos qubits

$$
\begin{aligned}
|\psi_2\rangle_{CAB} = \tfrac{1}{2}[&|00\rangle_{CA}(\alpha|0\rangle + \beta|1\rangle)_B + \\
&|01\rangle_{CA}(\alpha|1\rangle + \beta|0\rangle)_B + \\
&|10\rangle_{CA}(\alpha|0\rangle - \beta|1\rangle)_B + \\
&|11\rangle_{CA}(\alpha|1\rangle - \beta|0\rangle)_B]
\end{aligned}
$$

Teleportación cuántica

El algoritmo

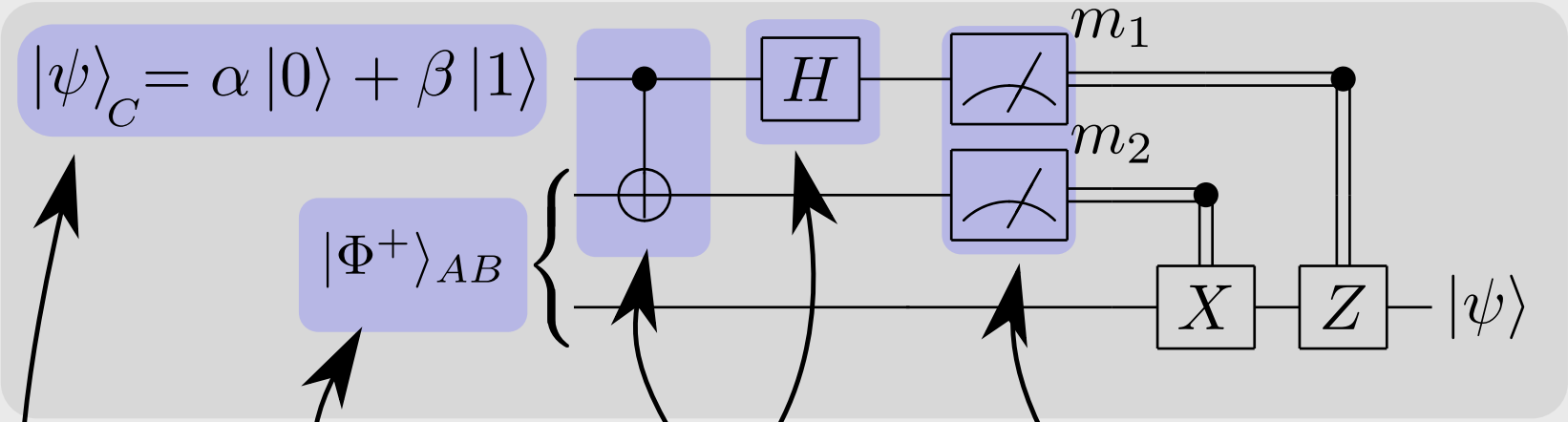


Bob recupera el estado inicial (a menos de una rotación)

$$
\begin{aligned}
|\psi_2\rangle_{CAB} = \tfrac{1}{2}[&|00\rangle_{CA}(\alpha|0\rangle + \beta|1\rangle)_B + \\
&|01\rangle_{CA}(\alpha|1\rangle + \beta|0\rangle)_B + \\
&|10\rangle_{CA}(\alpha|0\rangle - \beta|1\rangle)_B + \\
&|11\rangle_{CA}(\alpha|1\rangle - \beta|0\rangle)_B]
\end{aligned}
$$

Teleportación cuántica

Preparación remota de estados cuánticos



Entrelazamiento
Fuente de fotones entrelazados en polarización

CNOT
En camino y polarización

Hadamard
En camino

Medidas proyectivas
Tomografía de estados cuánticos

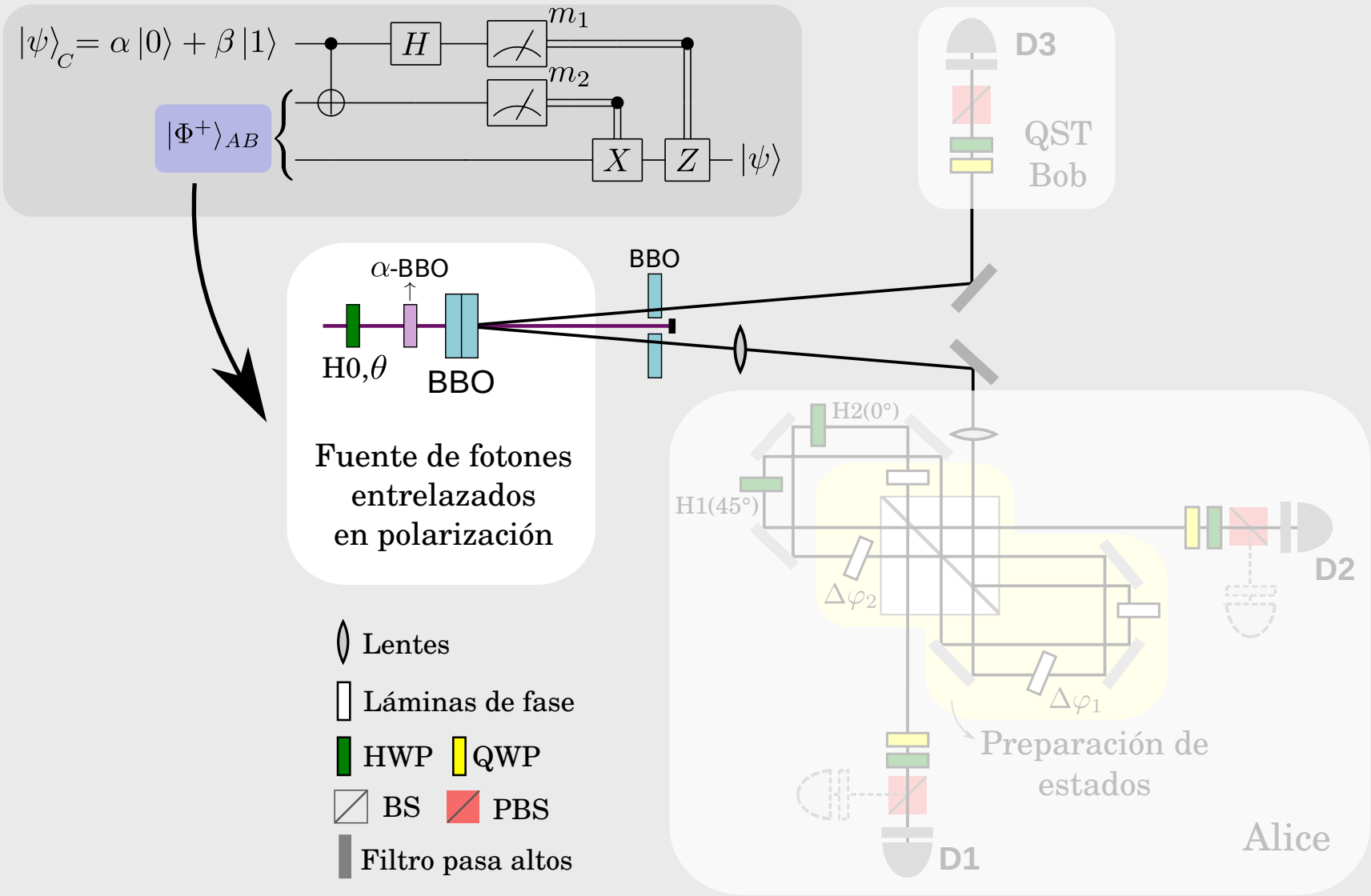
Estado de entrada
Codificado en el camino de un fotón

2 Fotones (SPDC)
↓
3 qubits
- polarización de 2 fotones
- camino de 1 fotón

D Bouwmeester, Nature 390 (1997)
D Boschi, Phys. Rev. Lett. 80 (1998)
JW Pan, Nature 518 (2015) & Nature 549 (2017)

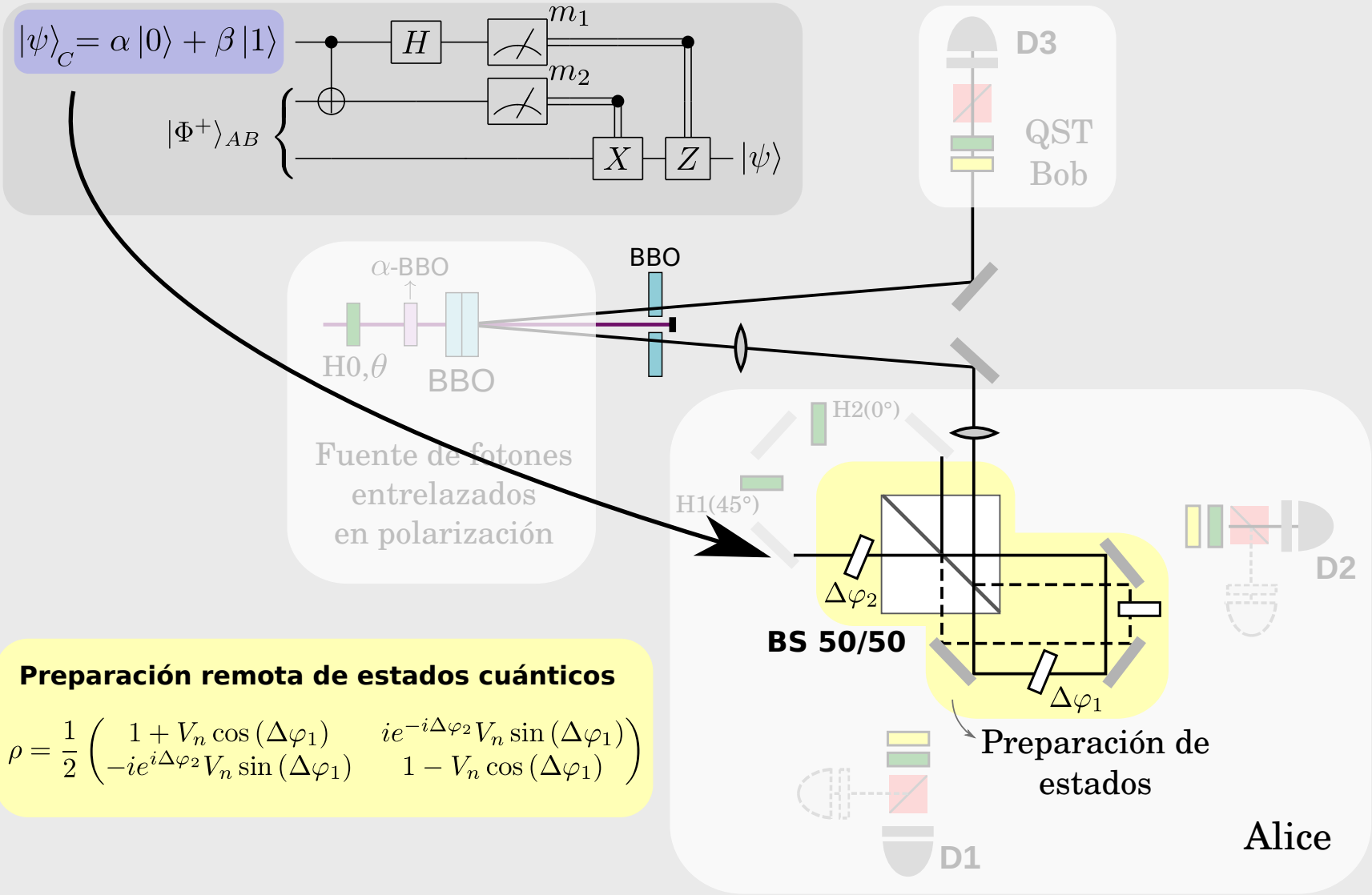
Teleportación cuántica

Implementación fotónica



Teleportación cuántica

Implementación fotónica

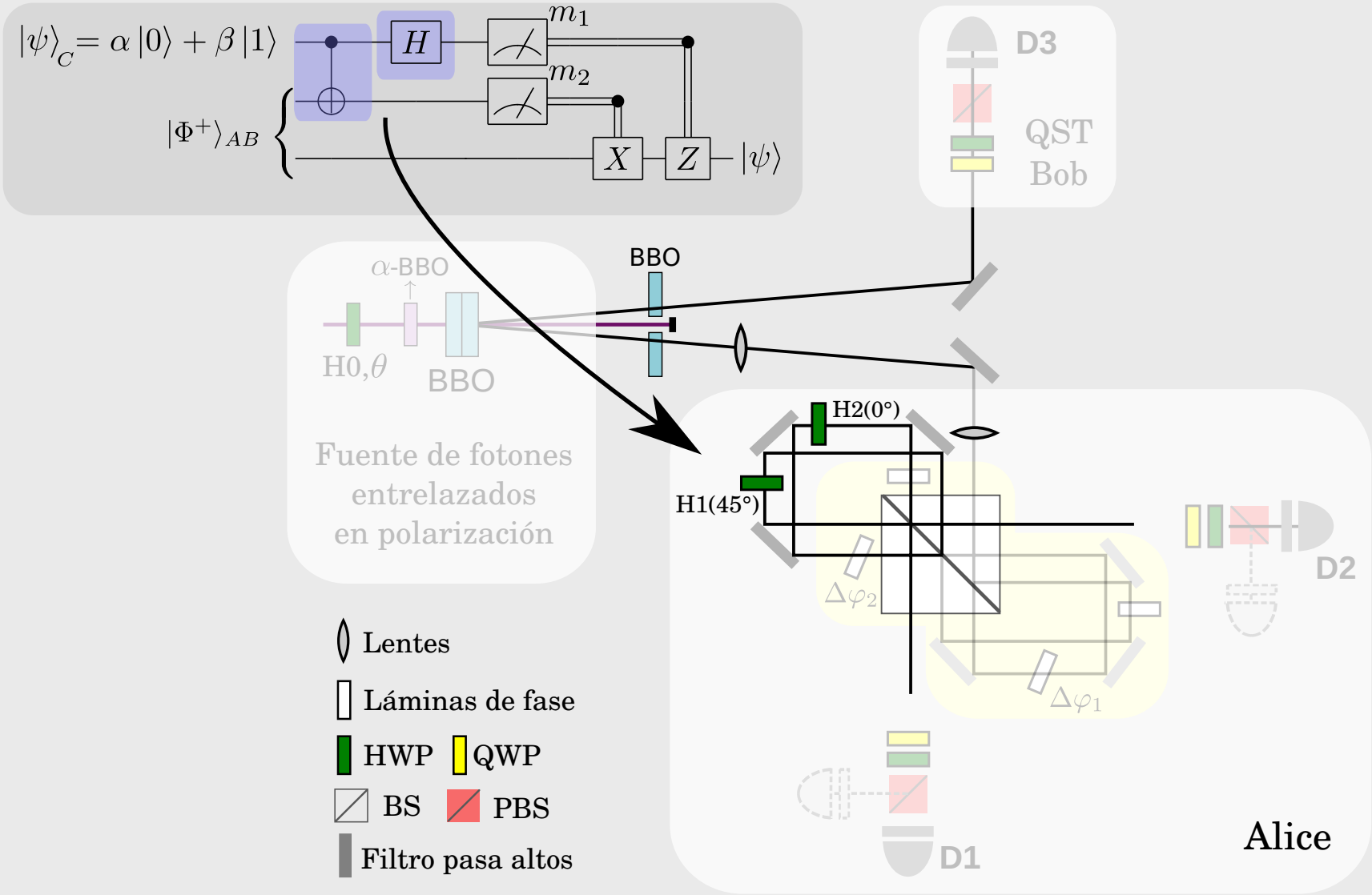


Preparación remota de estados cuánticos

$$\rho = \frac{1}{2}\begin{pmatrix} 1 + V_n \cos(\Delta\varphi_1) & ie^{-i\Delta\varphi_2} V_n \sin(\Delta\varphi_1) \\ -ie^{i\Delta\varphi_2} V_n \sin(\Delta\varphi_1) & 1 - V_n \cos(\Delta\varphi_1) \end{pmatrix}$$

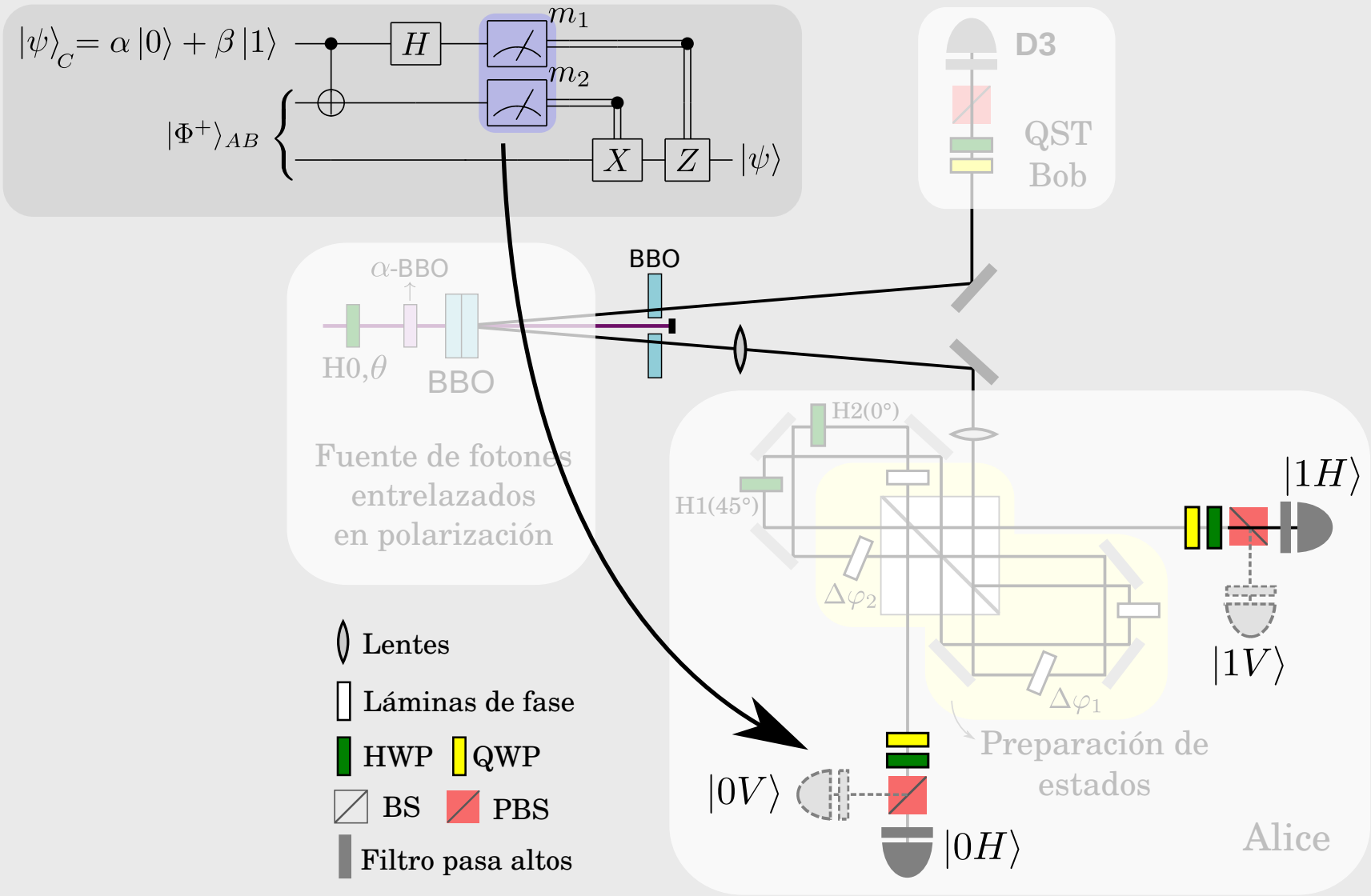
Teleportación cuántica

Implementación fotónica



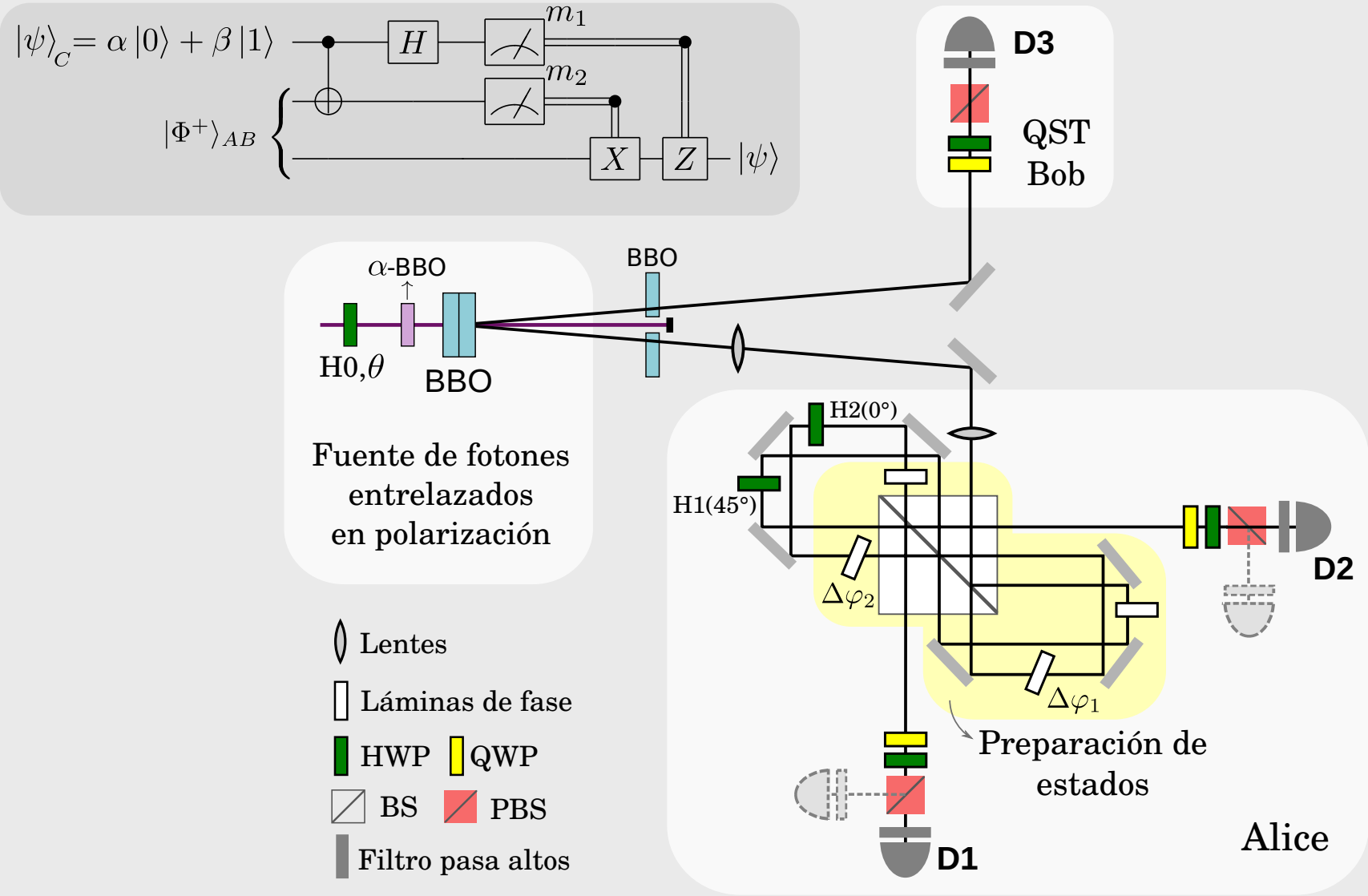
Teleportación cuántica

Implementación fotónica



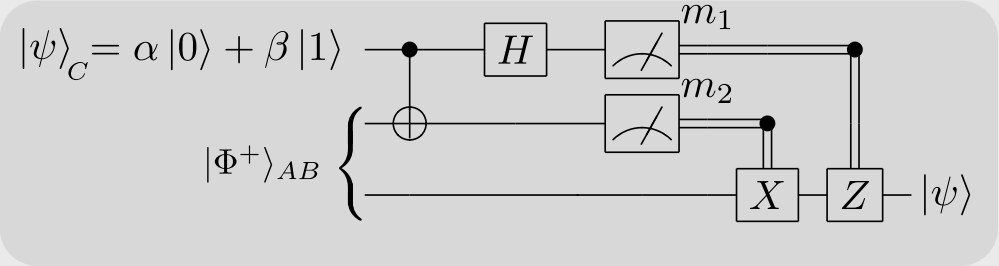
Teleportación cuántica

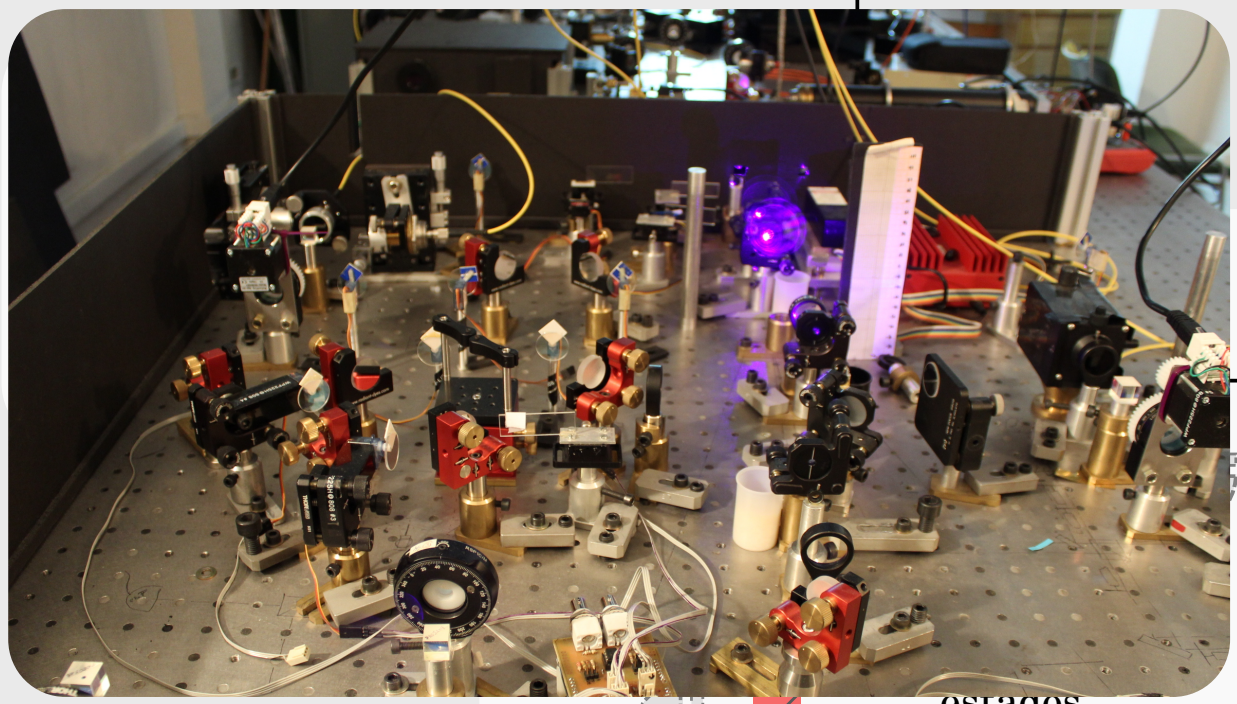
Implementación fotónica

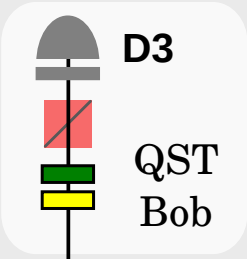


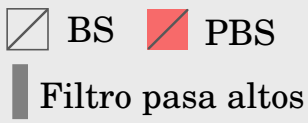
Teleportación cuántica

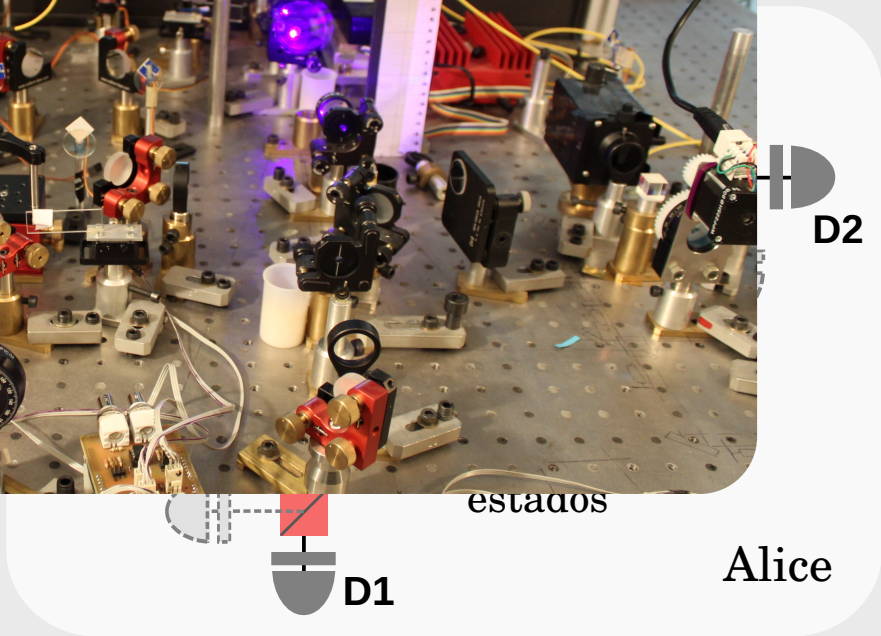
Implementación fotónica





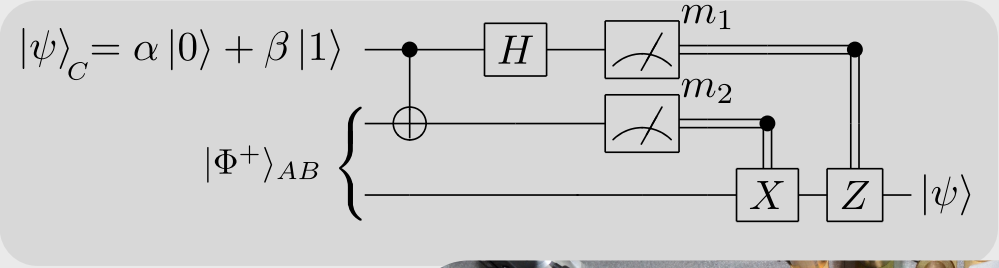


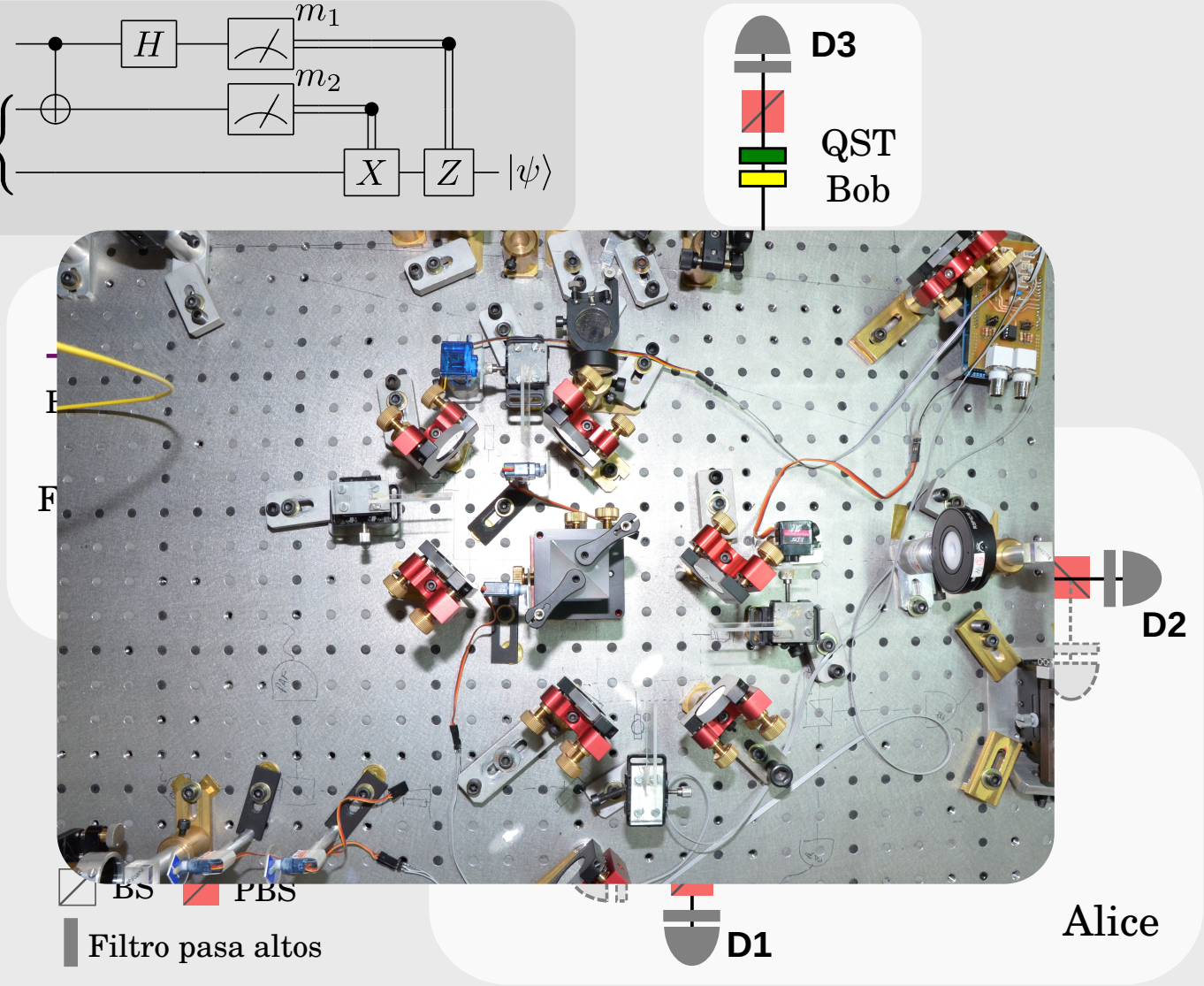




Teleportación cuántica

Implementación fotónica



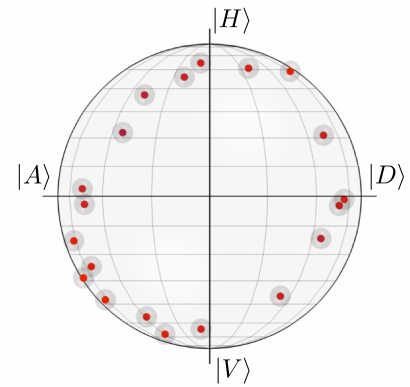


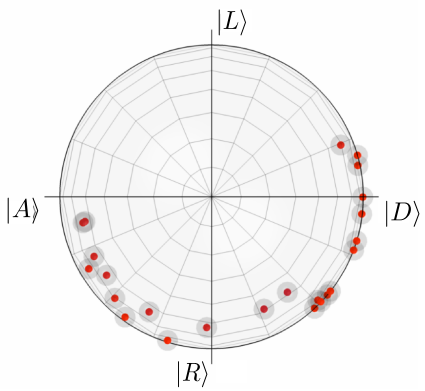
Teleportación cuántica

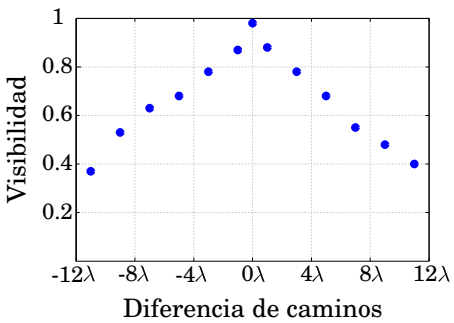
Implementación fotónica

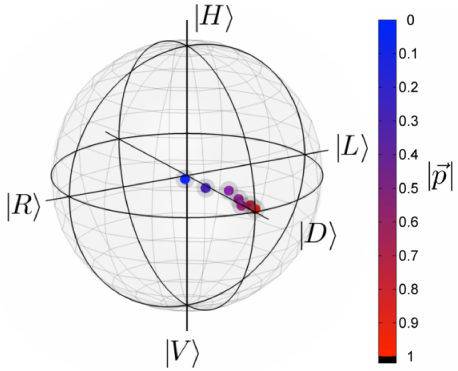
Preparación remota de estados cuánticos

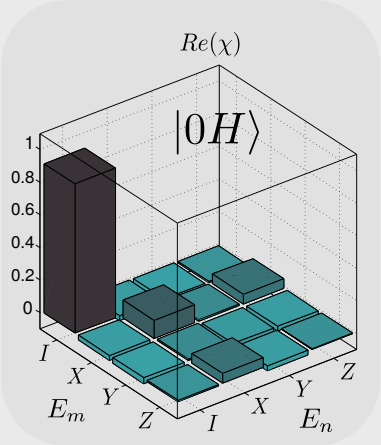
$$\rho = \frac{1}{2}\begin{pmatrix} 1 + V_n \cos(\Delta\varphi_1) & ie^{-i\Delta\varphi_2} V_n \sin(\Delta\varphi_1) \\ -ie^{i\Delta\varphi_2} V_n \sin(\Delta\varphi_1) & 1 - V_n \cos(\Delta\varphi_1) \end{pmatrix}$$



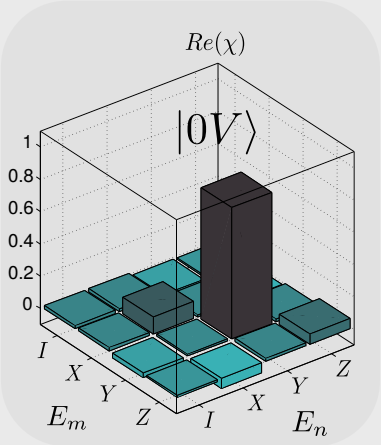




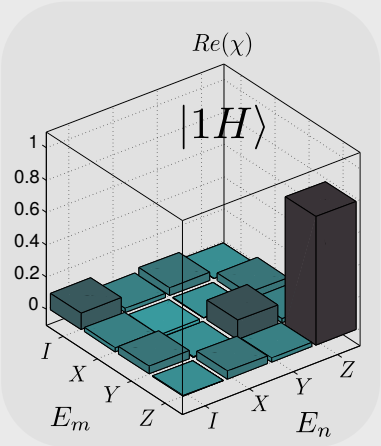




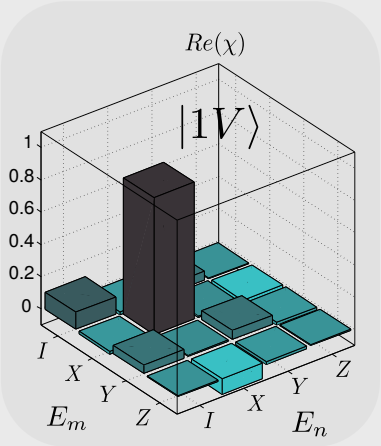
$F^I_{AV} = 0.95 \pm 0.02$



$F^Y_{AV} = 0.87 \pm 0.02$



$F^Z_{AV} = 0.87 \pm 0.02$



$F^X_{AV} = 0.90 \pm 0.02$

Knoll, Schmiegelow, Larotonda, App. Phys. B 115 (2014)

Estructura de la charla

Introducción

- Generación de pares de fotones entrelazados en polarización
- Codificación de qubits en grados de libertad de un fotón

Teleportación cuántica

- Implementación fotónica y resultados

Distribución cuántica de claves

- Implementación fotónica
- Espionaje con una máquina de clonación

Distribución cuántica de claves

Protocolo BB84 con entrelazamiento

Generación de la clave

ALICE ← ✳ → **BOB**

$\{+,\times\}$ $|\Phi^+\rangle$ $\{+,\times\}$

$+$ (computacional)

$0 \Leftrightarrow |H\rangle = \frac{1}{\sqrt{2}}(|D\rangle + |A\rangle)$

$1 \Leftrightarrow |V\rangle = \frac{1}{\sqrt{2}}(|D\rangle - |A\rangle)$

$\times$ (diagonal)

$0 \Leftrightarrow |D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$

$1 \Leftrightarrow |A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$

Alice: Elección aleatoria de base de detección.

Bob: Elección aleatoria de base de detección.

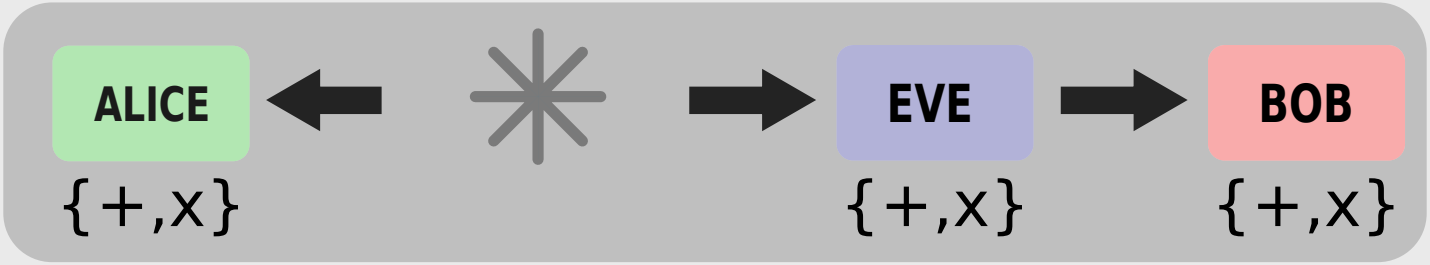
Alice publica las bases

Bob las coincidencias de bases

Bases Alice	+	×	+	+	×	×	×	+
Bits Alice	1	0	0	1	1	0	1	0
Bases Bob	×	×	+	×	+	+	×	+
Bits Bob	0	0	0	1	0	1	1	0
Coincidencias		✓	✓				✓	✓
Clave tamizada		0	0				1	0

Distribución cuántica de claves

Protocolo BB84 con entrelazamiento



B_A (Bases de Alice)	+	×	+	×	+	×
B_E (Bases de Eve)	× / +	× / +	+	×	×	+
B_B (Bases de Bob)	×	+	+	×	+	×
Efecto	✖				✖ 50% / 50% QBER ↑	

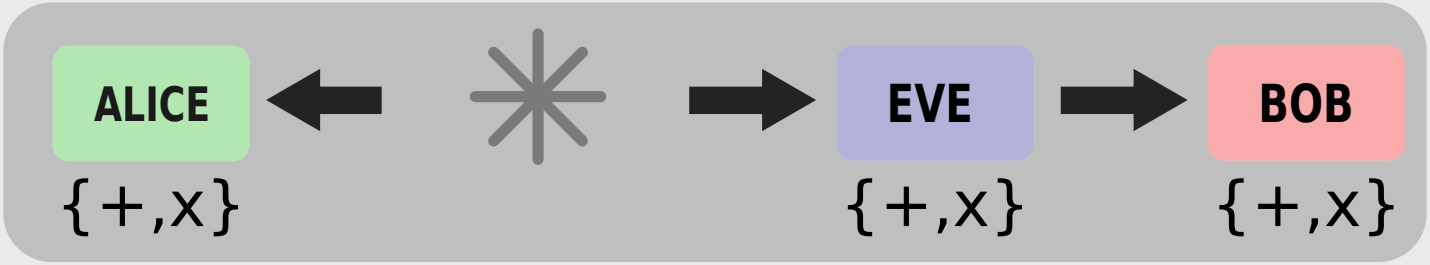
Intervención de un espía

- Intercepta los fotones
- Realiza un medida
- Reenvía a Bob el estado medido

CA Fuchs, Phys. Rev. A 56 (1997)
G Mauro D'Ariano, C Macchiavello, Phys. Rev. A 67 (2003)

Distribución cuántica de claves

Protocolo BB84 con entrelazamiento



B_A (Bases de Alice)	+	×	+	×	+	×
B_E (Bases de Eve)	× / +	× / +	+	×	×	+
B_B (Bases de Bob)	×	+	+	×	+	×
Efecto	✖				✖ 50% / 50% QBER ↑	

Se descartan de la clave tamizada

Eve no perturba el qubit

Genera errores en la clave tamizada !

Intervención de un espía

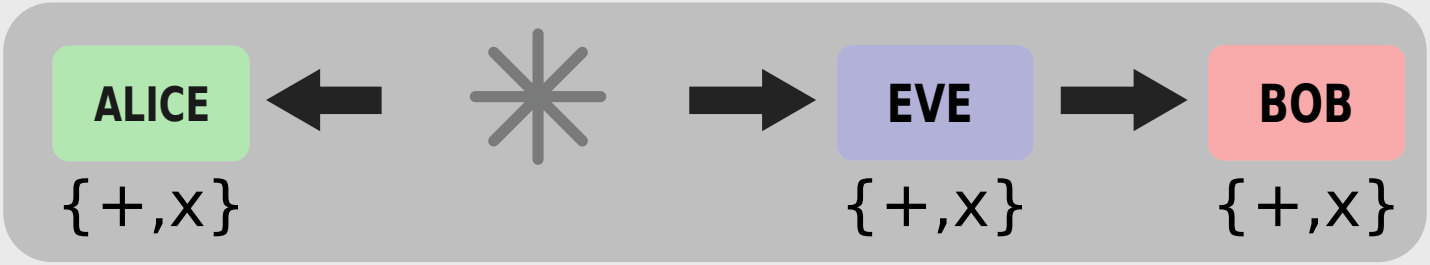
- Intercepta los fotones
- Realiza un medida
- Reenvía a Bob el estado medido

QBER: 25%

CA Fuchs, Phys. Rev. A 56 (1997)
G Mauro D'Ariano, C Macchiavello, Phys. Rev. A 67 (2003)

Distribución cuántica de claves

Protocolo BB84 con entrelazamiento



B_A (Bases de Alice)	+	×	+	×	+	×
B_E (Bases de Eve)	× / +	× / +	+	×	×	+
B_B (Bases de Bob)	×	+	+	×	+	×
Efecto	✖				✖ 50% / 50% QBER ↑	

Se descartan de la clave tamizada

Eve no perturba el qubit

Genera errores en la clave tamizada !

Intervención de un espía

- Intercepta los fotones
- Realiza un medida
- Reenvía a Bob el estado medido

QBER: 25%

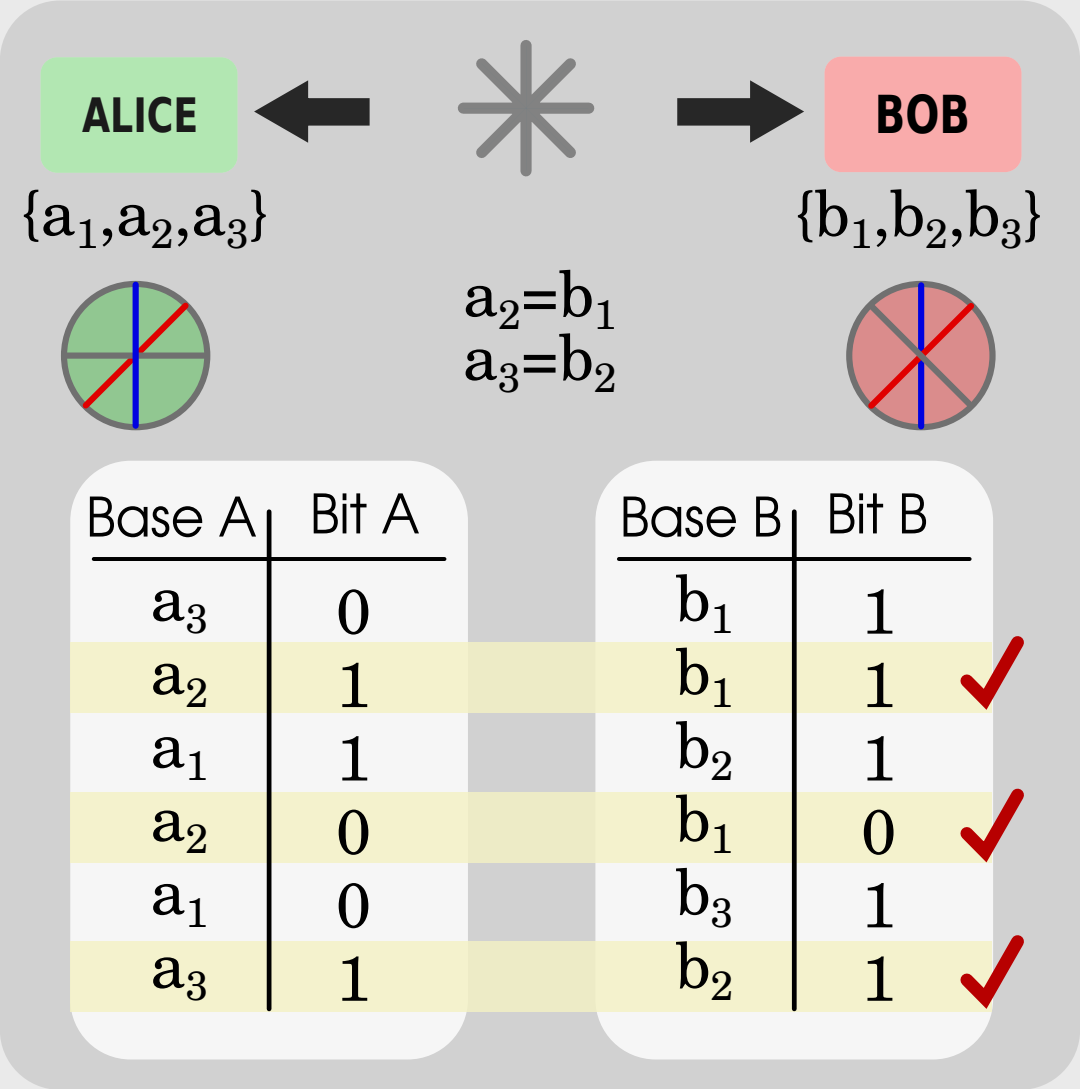
Ataque óptimo: Clonación de estados *(phase covariant cloning)*

QBER: 15%

CA Fuchs, Phys. Rev. A 56 (1997)
G Mauro D'Ariano, C Macchiavello, Phys. Rev. A 67 (2003)

Distribución cuántica de claves

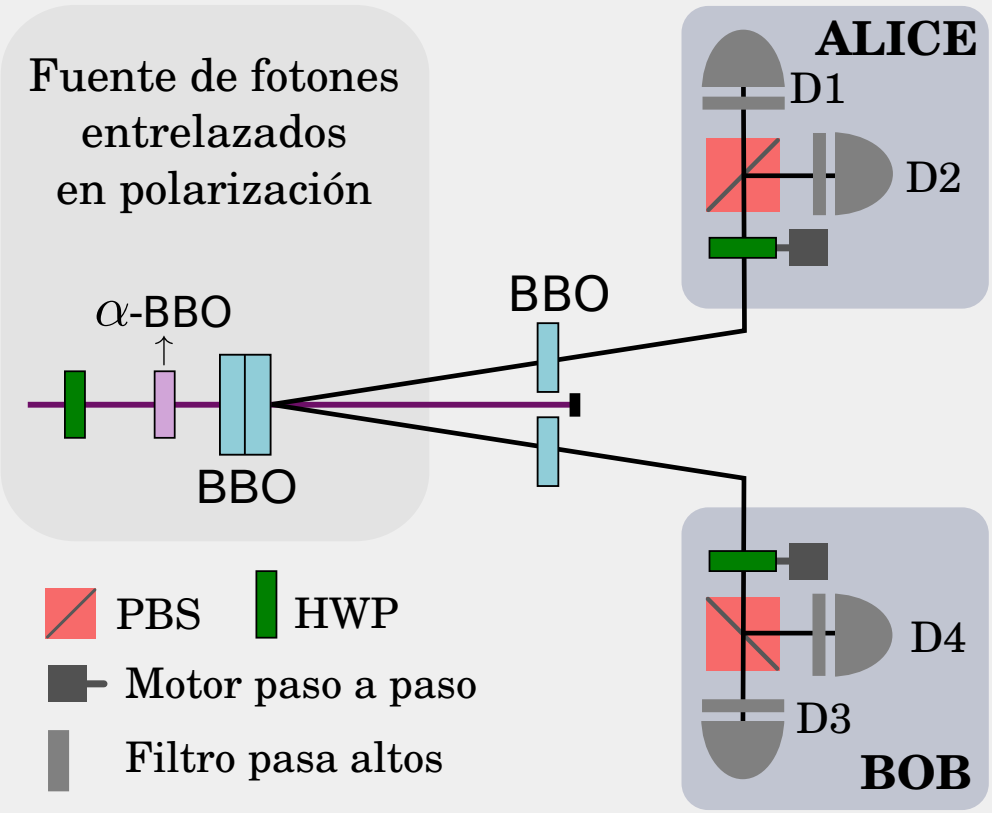
Protocolo E91

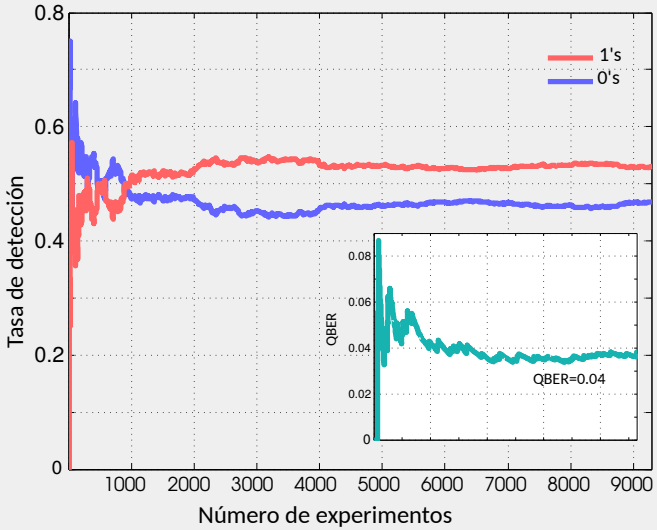


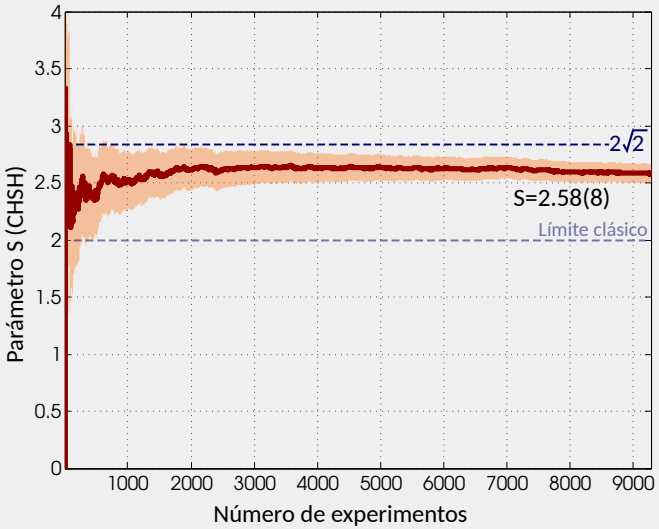
Base A	Bit A
a_3	0
a_2	1
a_1	1
a_2	0
a_1	0
a_3	1

Base B	Bit B	
b_1	1	
b_1	1	✓
b_2	1	
b_1	0	✓
b_3	1	
b_2	1	✓

Implementación del protocolo E91 de QKD







Clonación de estados cuánticos

Máquina de clonación universal (UQCM) vs *Phase Covariant Cloning* (PCC)

- La UQCM óptima puede alcanzar una fidelidad F=5/6=0.833
- Las máquinas de clonacón dependientes del estado pueden alcanzar fidelidades mayores a la UQCM para ciertos estados restringidos
- La *phase-covariant QCM* es capaz de clonar de manera óptima los estados sobre el ecuador de la esfera de Bloch: $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$

V Buzek, M Hillery, Phys. Rev. A, 54(3) (1996)
CS Niu, RB Griffiths, Phys. Rev. A 60 (1999)

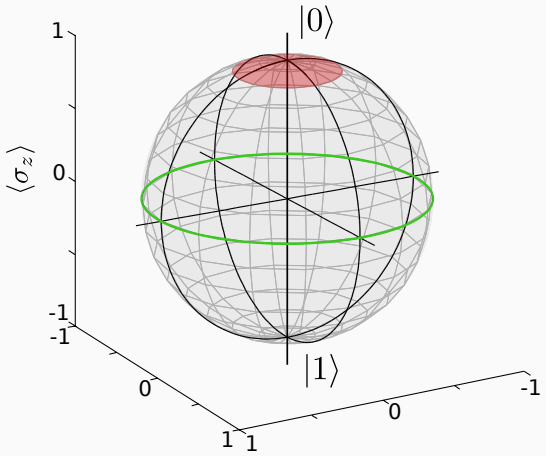
Clonación de estados cuánticos

Máquina de clonación universal (UQCM) vs *Phase Covariant Cloning* (PCC)

- La UQCM óptima puede alcanzar una fidelidad F=5/6=0.833
- Las máquinas de clonacón dependientes del estado pueden alcanzar fidelidades mayores a la UQCM para ciertos estados restringidos
- La *phase-covariant QCM* es capaz de clonar de manera óptima los estados sobre el ecuador de la esfera de Bloch: $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$

PCCM asimétrica

$$\text{PCC(+)} \begin{cases} |0\rangle_B|0\rangle_E \rightarrow |0\rangle_B|0\rangle_E \\ |1\rangle_B|0\rangle_E \rightarrow \sqrt{1-q}|1\rangle_B|0\rangle_E + \sqrt{q}|0\rangle_B|1\rangle_E \end{cases}$$



Clonación de estados cuánticos

Máquina de clonación universal (UQCM) vs *Phase Covariant Cloning* (PCC)

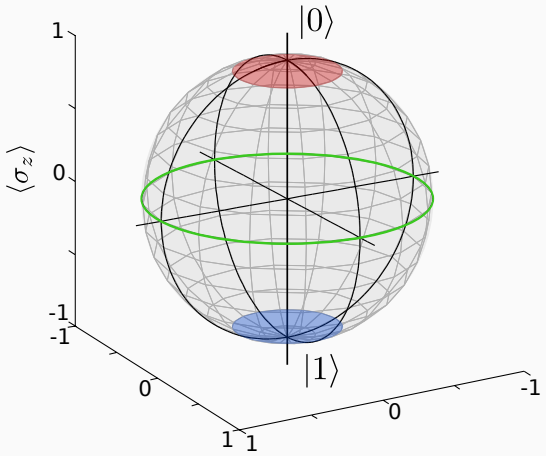
- La UQCM óptima puede alcanzar una fidelidad F=5/6=0.833
- Las máquinas de clonacón dependientes del estado pueden alcanzar fidelidades mayores a la UQCM para ciertos estados restringidos
- La *phase-covariant QCM* es capaz de clonar de manera óptima los estados sobre el ecuador de la esfera de Bloch: $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$

PCCM asimétrica

PCC(+) $\begin{cases} |0\rangle_B|0\rangle_E \rightarrow |0\rangle_B|0\rangle_E \\ |1\rangle_B|0\rangle_E \rightarrow \sqrt{1-q}|1\rangle_B|0\rangle_E + \sqrt{q}|0\rangle_B|1\rangle_E \end{cases}$

PCCM "espejada"

PCC(-) $\begin{cases} |1\rangle_B|0\rangle_E \rightarrow |1\rangle_B|0\rangle_E \\ |0\rangle_B|0\rangle_E \rightarrow \sqrt{1-q}|0\rangle_B|0\rangle_E + \sqrt{q}|1\rangle_B|1\rangle_E \end{cases}$



Clonación de estados cuánticos

Máquina de clonación universal (UQCM) vs *Phase Covariant Cloning* (PCC)

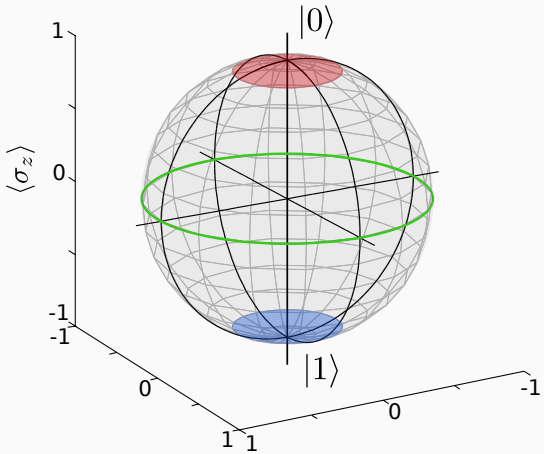
- La UQCM óptima puede alcanzar una fidelidad F=5/6=0.833
- Las máquinas de clonacón dependientes del estado pueden alcanzar fidelidades mayores a la UQCM para ciertos estados restringidos
- La *phase-covariant QCM* es capaz de clonar de manera óptima los estados sobre el ecuador de la esfera de Bloch: $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$

PCCM asimétrica

PCC(+) $\begin{cases} |0\rangle_B|0\rangle_E \rightarrow |0\rangle_B|0\rangle_E \\ |1\rangle_B|0\rangle_E \rightarrow \sqrt{1-q}|1\rangle_B|0\rangle_E + \sqrt{q}|0\rangle_B|1\rangle_E \end{cases}$

PCCM "espejada"

PCC(-) $\begin{cases} |1\rangle_B|0\rangle_E \rightarrow |1\rangle_B|0\rangle_E \\ |0\rangle_B|0\rangle_E \rightarrow \sqrt{1-q}|0\rangle_B|0\rangle_E + \sqrt{q}|1\rangle_B|1\rangle_E \end{cases}$

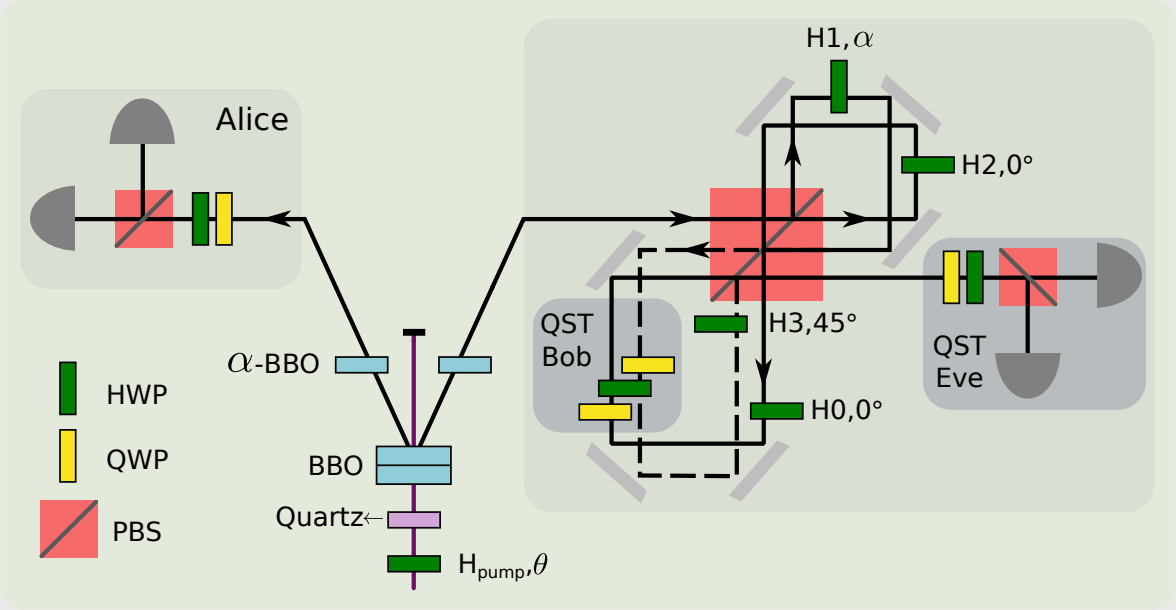


Fidelidad de los clones, para estados sobre el ecuador de la esfera de Bloch:

$$F_B = \langle\psi|\rho_B|\psi\rangle = \frac{1}{2}(1+\sqrt{1-q}), F_E = \langle\psi|\rho_E|\psi\rangle = \frac{1}{2}(1+\sqrt{q})$$

Para el caso simétrico (q=0.5) se obtiene F_B=F_E=*0.8536*, superando la UQCM

Implementación fotónica
Arreglo Experimental



PCC(+) óptico:

$$|H\rangle|0\rangle \rightarrow |H\rangle|0\rangle$$
$$|V\rangle|0\rangle \rightarrow \sqrt{1-q}|V\rangle|0\rangle + \sqrt{q}|H\rangle|1\rangle$$

La asimetría de los clones es controlada por la HWP H1: $q = \sin^2(2\alpha)$

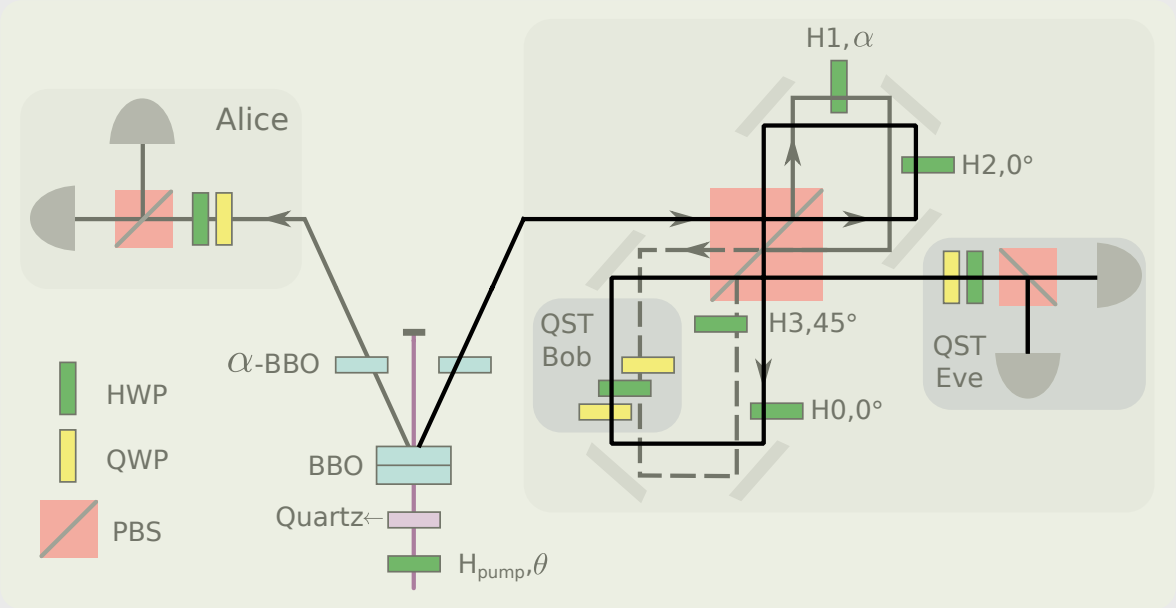
PCC(-) óptico:

$$|V\rangle|0\rangle \rightarrow |V\rangle|0\rangle$$
$$|H\rangle|0\rangle \rightarrow \sqrt{1-q}|H\rangle|0\rangle + \sqrt{q}|V\rangle|1\rangle$$

La asimetría de los clones es controlada por la HWP H2: $q = \sin^2(2\alpha')$

F Sciarrino, Phys. Rev. A 72 (2005)
J Soubusta, Phys. Rev. A 78 (2008)

Implementación fotónica
Arreglo Experimental



PCC(+) óptico:

$$|H\rangle|0\rangle \rightarrow |H\rangle|0\rangle$$
$$|V\rangle|0\rangle \rightarrow \sqrt{1-q}|V\rangle|0\rangle + \sqrt{q}|H\rangle|1\rangle$$

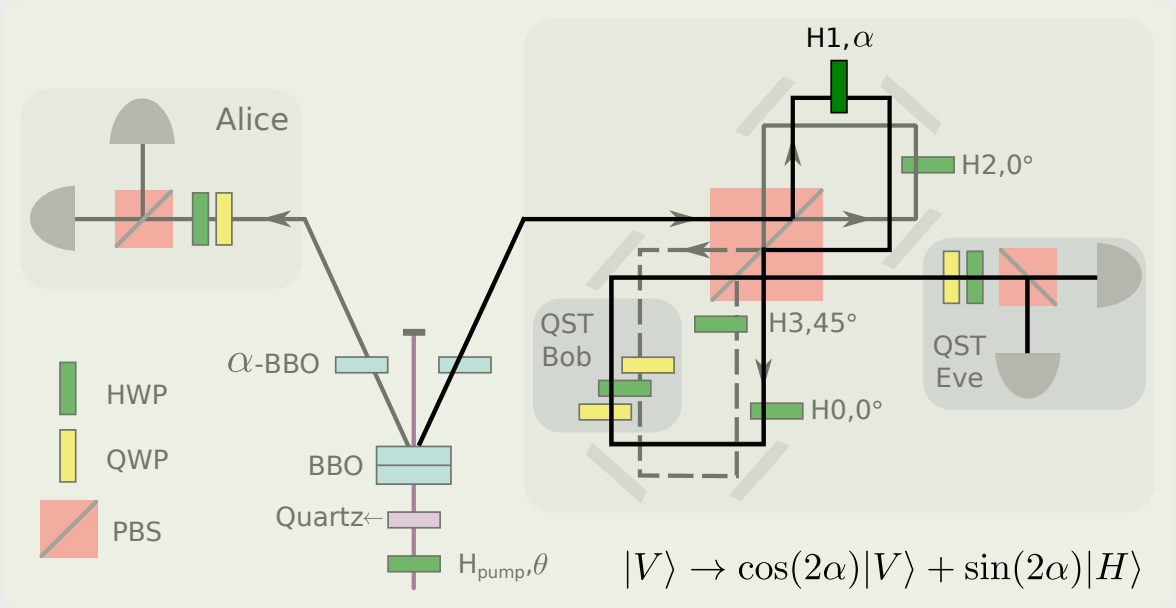
La asimetría de los clones es controlada por la HWP H1: $q = \sin^2(2\alpha)$

PCC(-) óptico:

$$|V\rangle|0\rangle \rightarrow |V\rangle|0\rangle$$
$$|H\rangle|0\rangle \rightarrow \sqrt{1-q}|H\rangle|0\rangle + \sqrt{q}|V\rangle|1\rangle$$

La asimetría de los clones es controlada por la HWP H2: $q = \sin^2(2\alpha')$

Implementación fotónica
Arreglo Experimental



PCC(+) óptico:

$$|H\rangle|0\rangle \rightarrow |H\rangle|0\rangle$$
$$|V\rangle|0\rangle \rightarrow \sqrt{1-q}|V\rangle|0\rangle + \sqrt{q}|H\rangle|1\rangle$$

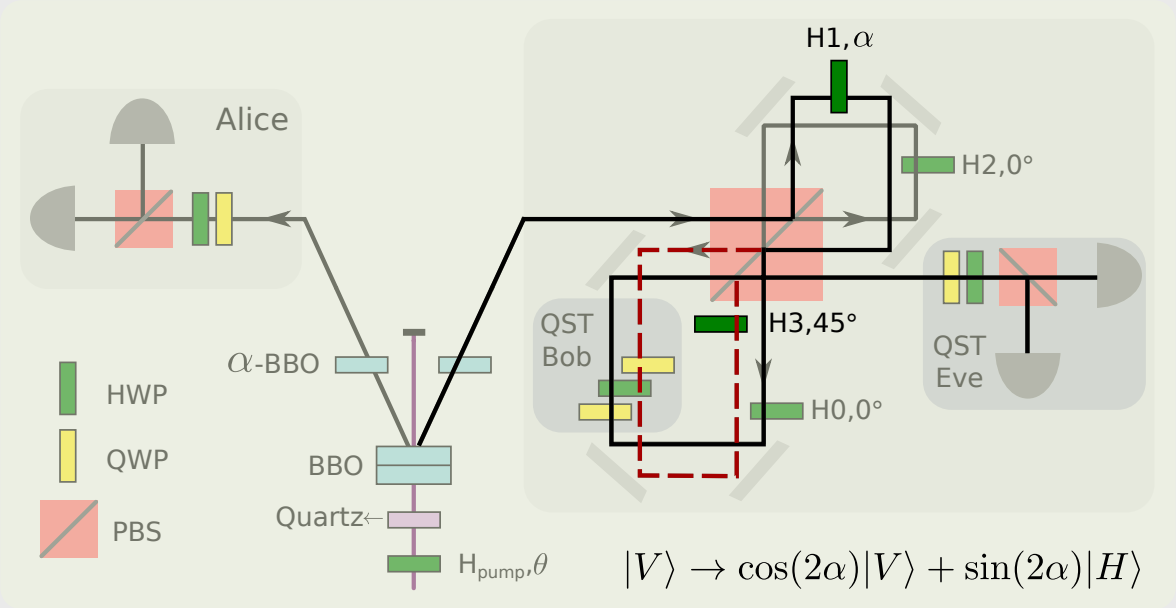
La asimetría de los clones es controlada por la HWP H1: $q = \sin^2(2\alpha)$

PCC(-) óptico:

$$|V\rangle|0\rangle \rightarrow |V\rangle|0\rangle$$
$$|H\rangle|0\rangle \rightarrow \sqrt{1-q}|H\rangle|0\rangle + \sqrt{q}|V\rangle|1\rangle$$

La asimetría de los clones es controlada por la HWP H2: $q = \sin^2(2\alpha')$

Implementación fotónica
Arreglo Experimental



PCC(+) óptico:

$$|H\rangle|0\rangle \rightarrow |H\rangle|0\rangle$$
$$|V\rangle|0\rangle \rightarrow \sqrt{1-q}|V\rangle|0\rangle + \boxed{\sqrt{q}|H\rangle|1\rangle}$$

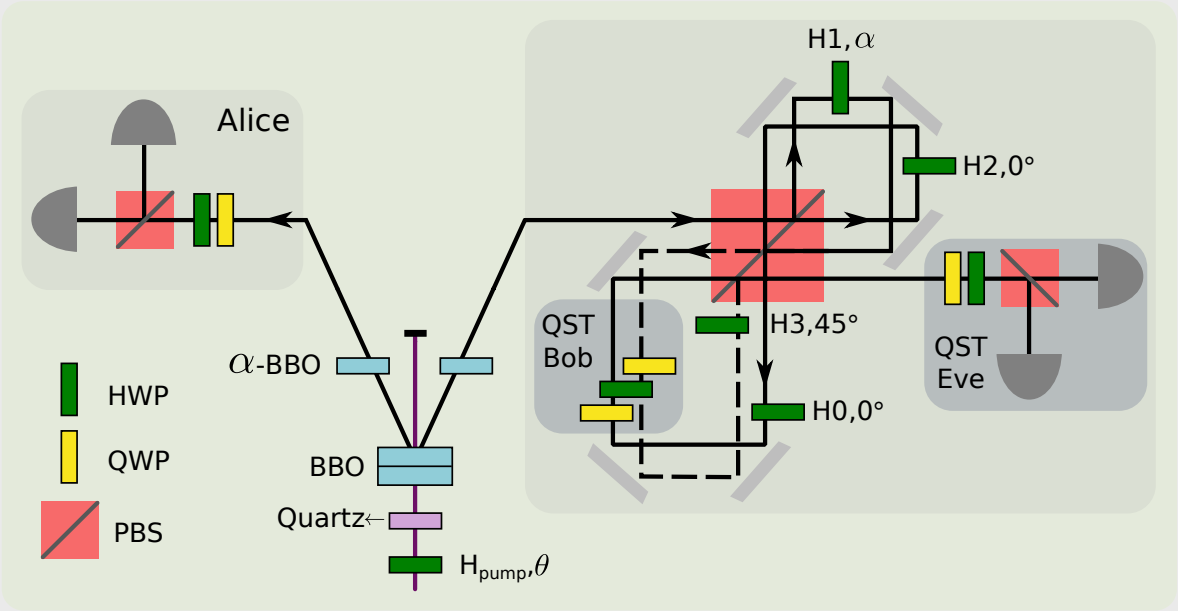
La asimetría de los clones es controlada por la HWP H1: $q = \sin^2(2\alpha)$

PCC(-) óptico:

$$|V\rangle|0\rangle \rightarrow |V\rangle|0\rangle$$
$$|H\rangle|0\rangle \rightarrow \sqrt{1-q}|H\rangle|0\rangle + \sqrt{q}|V\rangle|1\rangle$$

La asimetría de los clones es controlada por la HWP H2: $q = \sin^2(2\alpha')$

Implementación fotónica
Arreglo Experimental



- Alice y Bob comparten un estado entrelazado en polarización
- Eve está codificada en el qubit de camino del fotón de Bob
- Los fotones son detectados y enviados a un contador de coincidencias basado en una FPGA

PCC(+) óptico:

$$|H\rangle|0\rangle \rightarrow |H\rangle|0\rangle$$
$$|V\rangle|0\rangle \rightarrow \sqrt{1-q}|V\rangle|0\rangle + \sqrt{q}|H\rangle|1\rangle$$

La asimetría de los clones es controlada por la HWP H1: $q = \sin^2(2\alpha)$

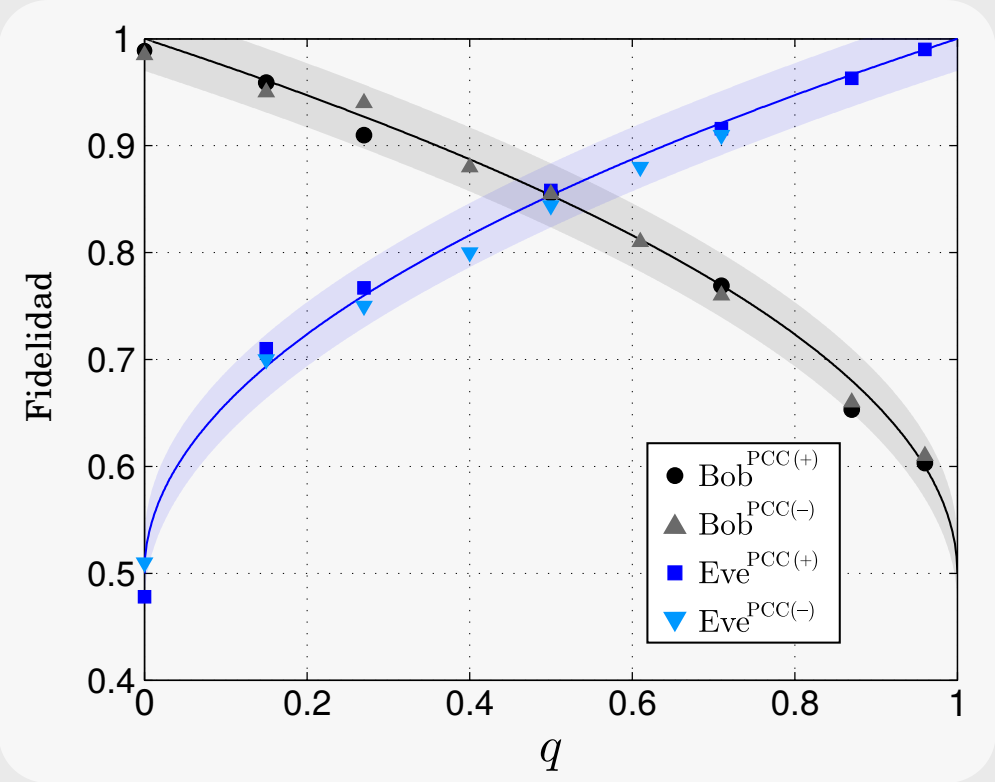
PCC(-) óptico:

$$|V\rangle|0\rangle \rightarrow |V\rangle|0\rangle$$
$$|H\rangle|0\rangle \rightarrow \sqrt{1-q}|H\rangle|0\rangle + \sqrt{q}|V\rangle|1\rangle$$

La asimetría de los clones es controlada por la HWP H2: $q = \sin^2(2\alpha')$

Resultados

Fidelidad de los clones para ambas máquinas PCC



- Alice proyecta su fotón al estado:

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

- Bob y Eve realizan tomografía cuántica de estados sobre sus qubits, para distintos parámetros de clonación

$$F_B = \langle\psi|\rho_B|\psi\rangle = \frac{1}{2}(1+\sqrt{1-q})$$
$$F_E = \langle\psi|\rho_E|\psi\rangle = \frac{1}{2}(1+\sqrt{q})$$

Para el caso simétrico en que *q=0.5* obtenemos un valor promedio de *F=0.852(5)*, superando a la UQCM.

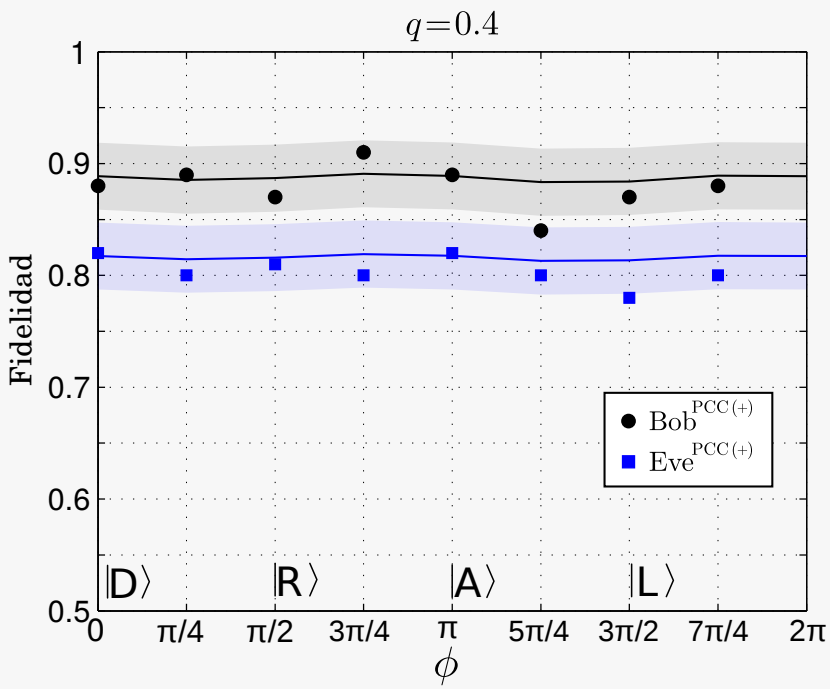
Resultados

Estados Ecuatoriales y No-Ecuatoriales

Fidelidad de los qubits de Bob y Eve, después de proyectar distintos estados del lado de Alice, para un valor particular del parámetro de clonación.

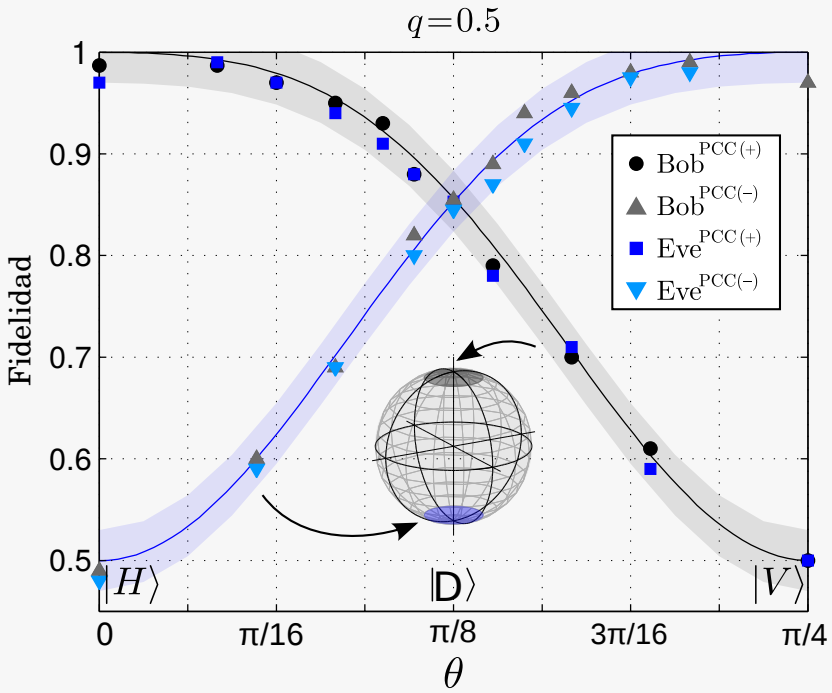
- **Estados Ecuatoriales**

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\phi}|V\rangle)$$

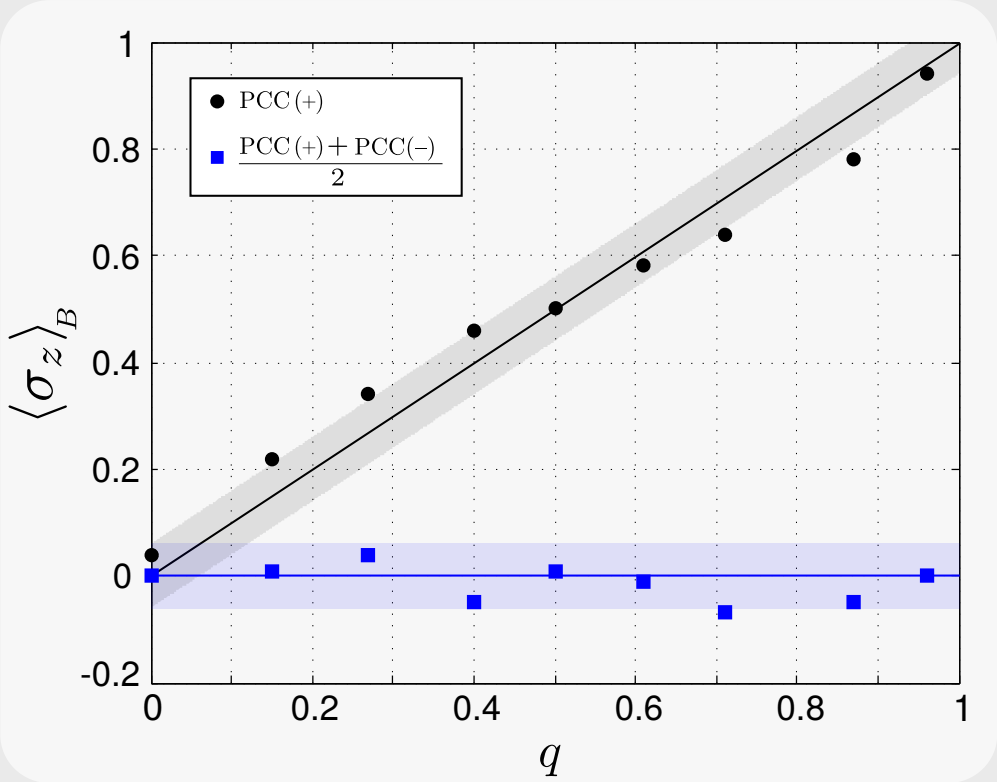


- **Estados No-Ecuatoriales**

$$|\psi\rangle = \cos(2\theta)|H\rangle + \sin(2\theta)|V\rangle$$



Resultados
Espionaje con PCC



- El límite de seguridad para el protocolo BB84 contra ataques incoherentes surge de situaciones en las que Eve utiliza una máquina PCC

- Un ataque por PCC introduce un sesgo en términos del parámetro q:

$$\langle\sigma_z\rangle = q$$

Knoll, Lopez Grande, Larotonda, App. Phys. B 124 (2018)

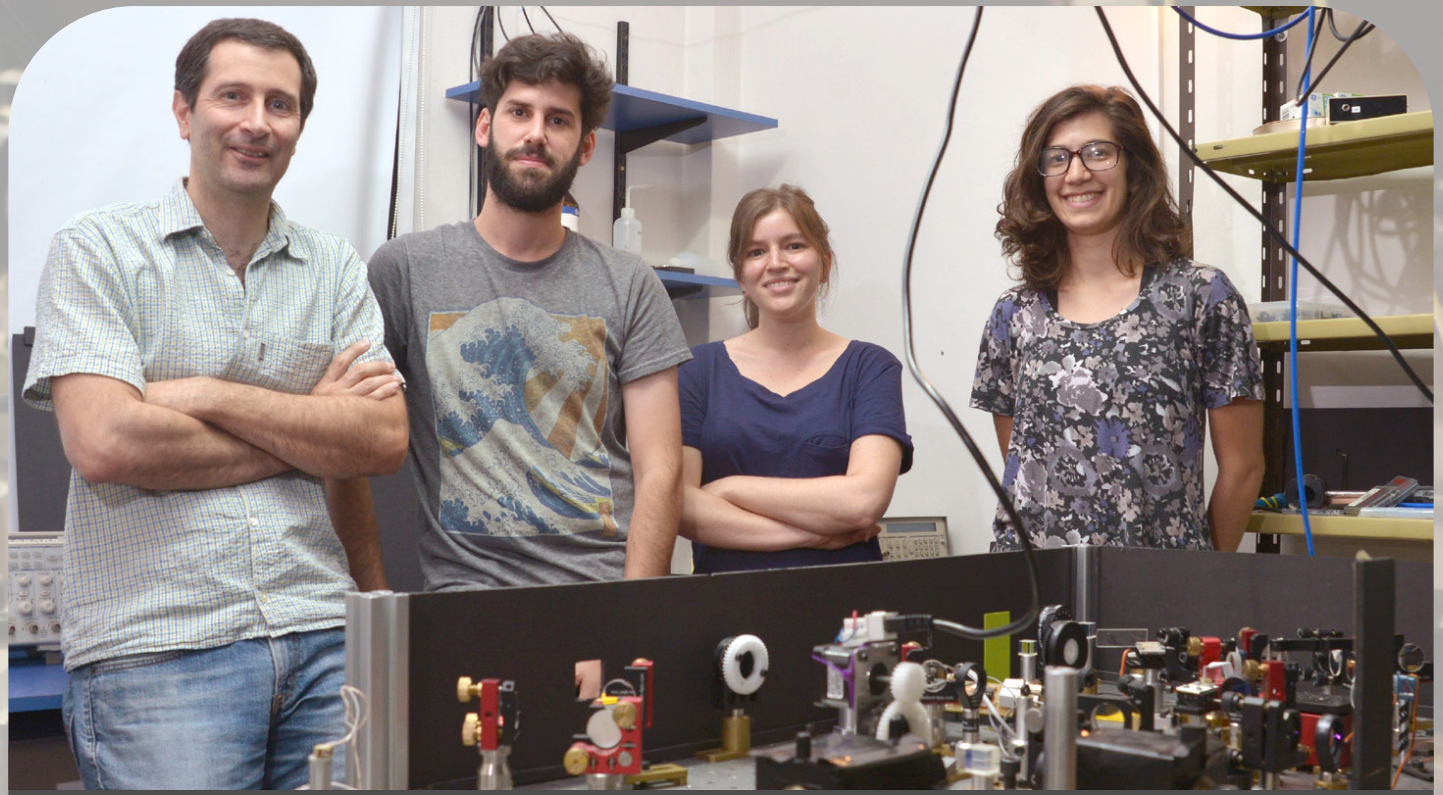
Al alternar entre ambas operaciones de clonación PCC(+) y PCC(-), Eve puede enmascarar su presencia enviando a Bob estados clonados sin sesgo en σ_z pero con la misma fidelidad individual.

Experimentos con fotones entrelazados
Resumiendo...

Generación y manipulación de qubits codificados en grados de libertad del fotón

Experimentos con fotones entrelazados:

- **Teleportación cuántica**
- **Distribución cuántica de claves (con y sin espía)**



Miguel Larotonda Ignacio López Grande Laura Knoll Agustina Magnoni

GRACIAS